User's Manual

IP7361 Network Camera

Outdoor · 2-megapixel · Day & Night

VIVOTEK

Table of Contents

Overview *3*

Read Before Use 3
Package Contents 3
Physical Description 4
Cabling Assembly 7
Hardware Installation 8
Network Deployment 10
Software Installation 13
Ready to Use 14
Accessories 16

Accessing the Network Camera *17*

Using Web Browsers 17
Using RTSP Players 19
Using 3GPP-compatible Mobile Devices 20
Using VIVOTEK Recording Software 21

Main Page *22*

Client Settings *26*

Configuration *28*

System 29
Security 31
HTTPS 32
SNMP 37
Network 38
DDNS 53
Access List 55
Audio and Video 58
Motion Detection 71
Camera Tampering Detection 74
Camera Control 75
Homepage Layout 82
Application 85
Recording 98
Local Storage 101
System Log 105
View Parameters 106
Maintenance 107

Appendix *111*

URL Commands for the Network Camera 111
Technical Specifications 168
Technology License Notice 169
Electromagnetic Compatibility (EMC) 170

Overview

VIVOTEK IP7361 is a high-end 2-megapixel network bullet camera surveillance. outdoor-specific features such as concealed wiring to prevent tampering, the IP7361 is the camera of choice for applications such as parking lots, gas stations, and building entrances.

The IP7361 boasts high-definition 2-megapixel (1600 x 1200) resolution, allowing for the delivery of extremely detailed images and coverage 6 times larger than a VGA camera. To maximize the benefit of the 2-megapixel sensor, the IP7361 employs several innovative technologies for optimized bandwidth efficiency. The ePTZ function enables users to quickly move to a target area for close-up shots without moving the camera physically. Users can also receive only the portions of the images they are interested in via the cropping function. Furthermore, multiple video streams can be delivered simultaneously in different resolutions, frame rates, and image qualities for viewing on different platforms so as to meet different needs or bandwidth constraints. The IP7361 also offers activity adaptive streaming support that dynamically allocates bandwidth according to the video content and trigger state.

Aimed at outdoor surveillance, the IP7361 features auto-iris capability to protect the lens from damage induced by direct sunlight. To adapt to light changes throughout the day, the camera is furnished with a removable IR-cut filter and IR illuminators for superior image quality around the clock. The IP7361 also comes with an IP67-rated housing that offers protection against rain and dust to ensure functional operation in all types of weather conditions. For easy management and protection against tempering and vandalism, the IP7361 is also equipped with a mounting bracket that conceals all cables within the bracket.

With other advanced features such as tamper detection, 802.3af compliant PoE, SD/SDHC card on-board storage, and two-way audio via SIP protocol, the IP7361 is a full-fledged surveillance solution for outdoor environments.

Read Before Use

The use of surveillance devices may be prohibited by law in your country. The Network Camera is not only a high-performance web-ready camera but can also be part of a flexible surveillance system. It is the user's responsibility to ensure that the operation of such devices is legal before installing this unit for its intended use.

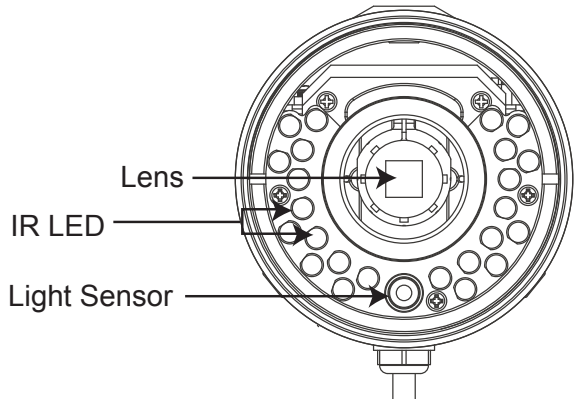
It is important to first verify that all contents received are complete according to the Package Contents listed below. Take note of the warnings in the Quick Installation Guide before the Network Camera is installed; then carefully read and follow the instructions in the Installation chapter to avoid damage due to faulty assembly and installation. This also ensures the product is used properly as intended.

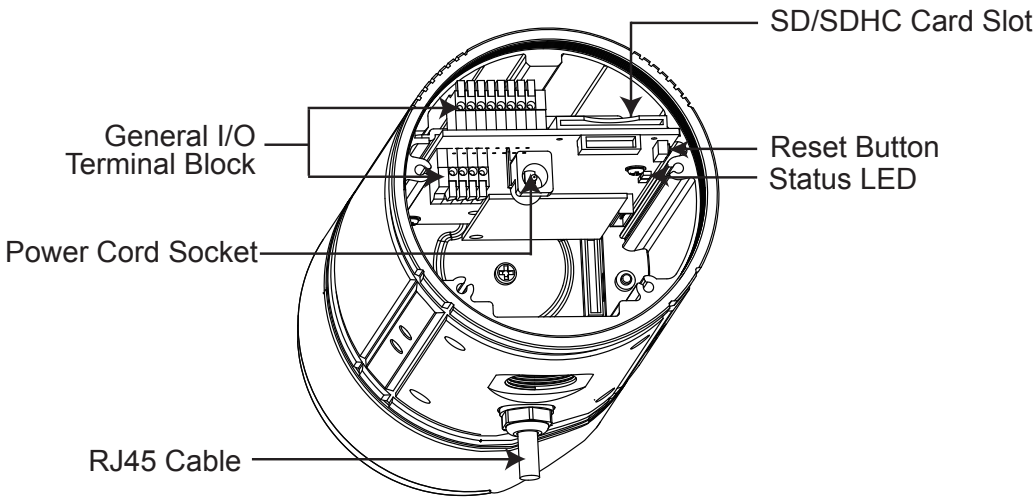
The Network Camera is a network device and its use should be straightforward for those who have basic networking knowledge. It is designed for various applications including video sharing, general security/ surveillance, etc. The Configuration chapter suggests ways to best utilize the Network Camera and ensure proper operations. For creative and professional developers, the URL Commands of the Network Camera section serves as a helpful reference to customizing existing homepages or integrating with the current web server.

Package Contents

- IP7361 with an RJ45 Cable
- Sun Shield
- Wall Mount Bracket
- Waterproof Connector for RJ45 Ethernet Enclosure
- Power Adapter
- Alignment Sticker / Silica Gel
- Waterproof Connector (for backup use)
- Software CD
- Quick Installation Guide / Warranty Card

Physical Description

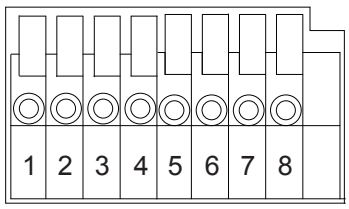




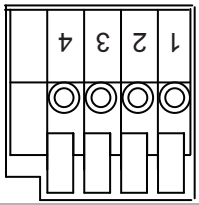
General I/O Terminal Block

This Network Camera provides a general I/O terminal block which is used to connect external input / output devices. The pin definitions are described below.

Pin	Name
1	Power +12V
2	Digital Output
3	Digital Input
4	Ground
5	AC 24V Input
6	AC 24V Input
7	RS-485 +
8	RS-485 -

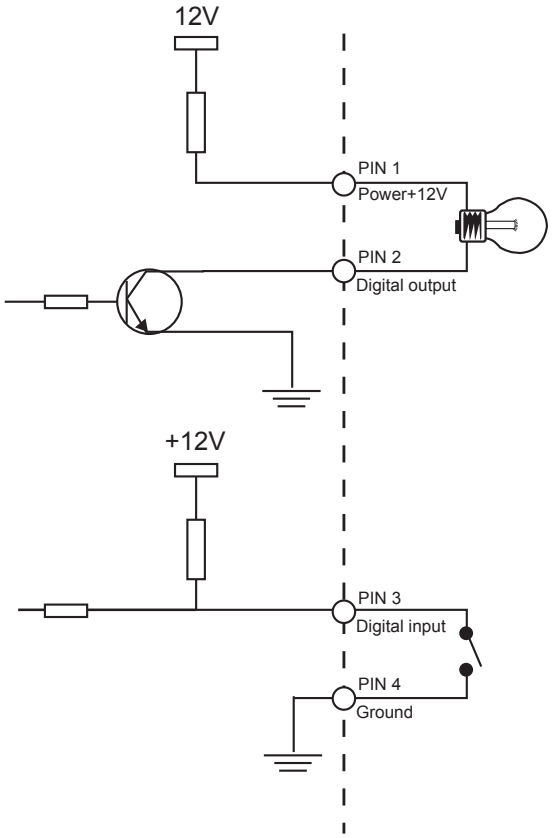


Pin	Name
1	External MIC In
2	Ground
3	Audio Out
4	Ground



DI/DO Diagram

Please refer to the following illustration for the connection method.

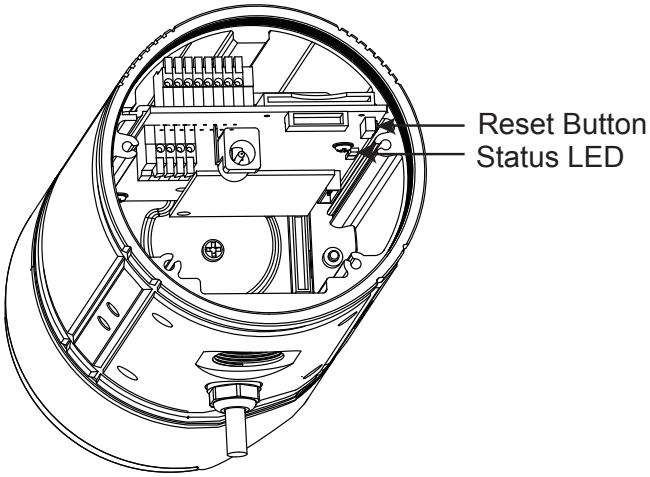


Status LED

The LED indicates the status of the Network Camera.

Item	LED status	Description
1	Steady Red	Power on and system booting
	Red LED unlighted	Power off
2	Steady Red + Blink Green every 1 sec.	Network works (heartbeat)
	Steady Red + Green LED unlighted	Network fail
3	Steady Red + Blink Green every 2 sec.	Audio mute (heartbeat)
4	Blink Red every 0.15 sec. + Blink Green every 1 sec.	Upgrading Firmware
5	Blink Red every 0.15 sec. + Blink Green every 0.15 sec.	Restore default

Hardware Reset



The reset button is used to reset the system or restore the factory default settings. Sometimes resetting the system can return the camera to normal operation. If the system problems remain after reset, restore the factory settings and install again.

Reset: Press and release the recessed reset button with a paper clip or thin object. Wait for the Network Camera to reboot.

Restore: Press and hold the recessed reset button until the status LED rapidly blinks. It takes about 30 seconds. Note that all settings will be restored to factory default. Upon successful restore, the status LED will blink green and red during normal operation.

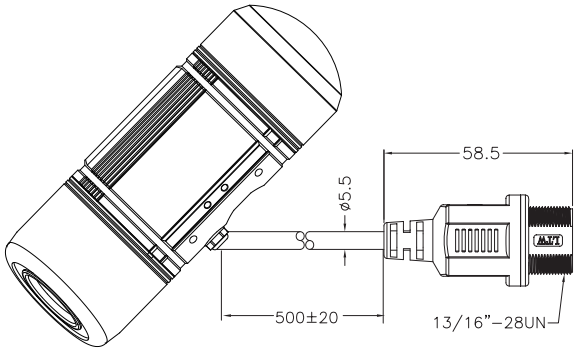
SD/SDHC Card Capacity

This network camera is compliant with **SD/SDHC 16GB / 8GB** and other preceding standard SD cards.

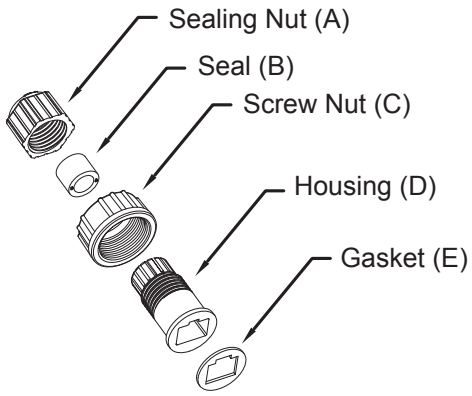
Cabling Assembly

RJ45 Cable Connector

RJ45 Cable Dimension (unit: mm)

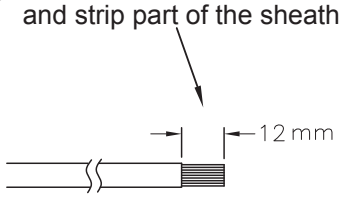


Components of the Waterproof Connector



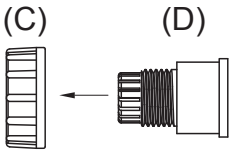
Assembling Steps

1. Prepare an Ethernet cable and strip part of the sheath.

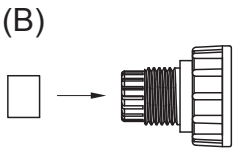


Recommended cable gauge: 24AWG (0.51 mm)

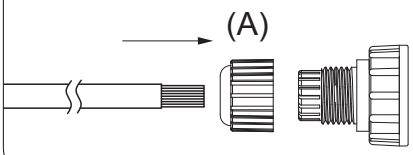
2. Insert the housing into the screw nut.



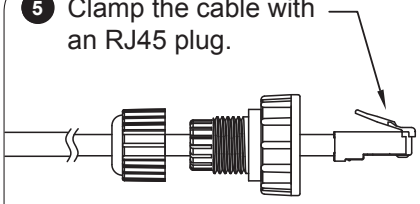
3. Insert the seal into the housing.



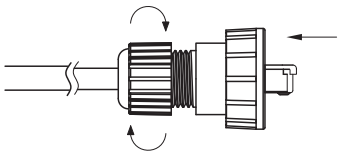
4. Insert the stripped Ethernet cable through the sealing nut and the housing.



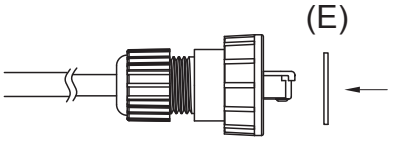
5. Clamp the cable with an RJ45 plug.



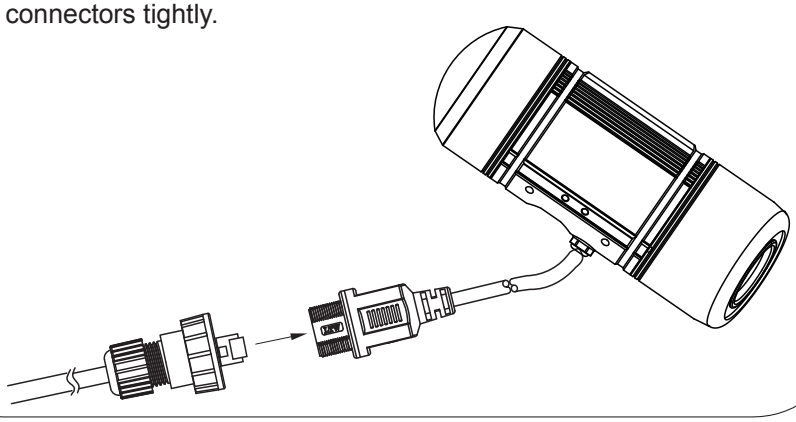
6. Push the RJ45 plug into the housing, then secure the sealing nut tightly.



7. Attach the gasket to the front of the housing.

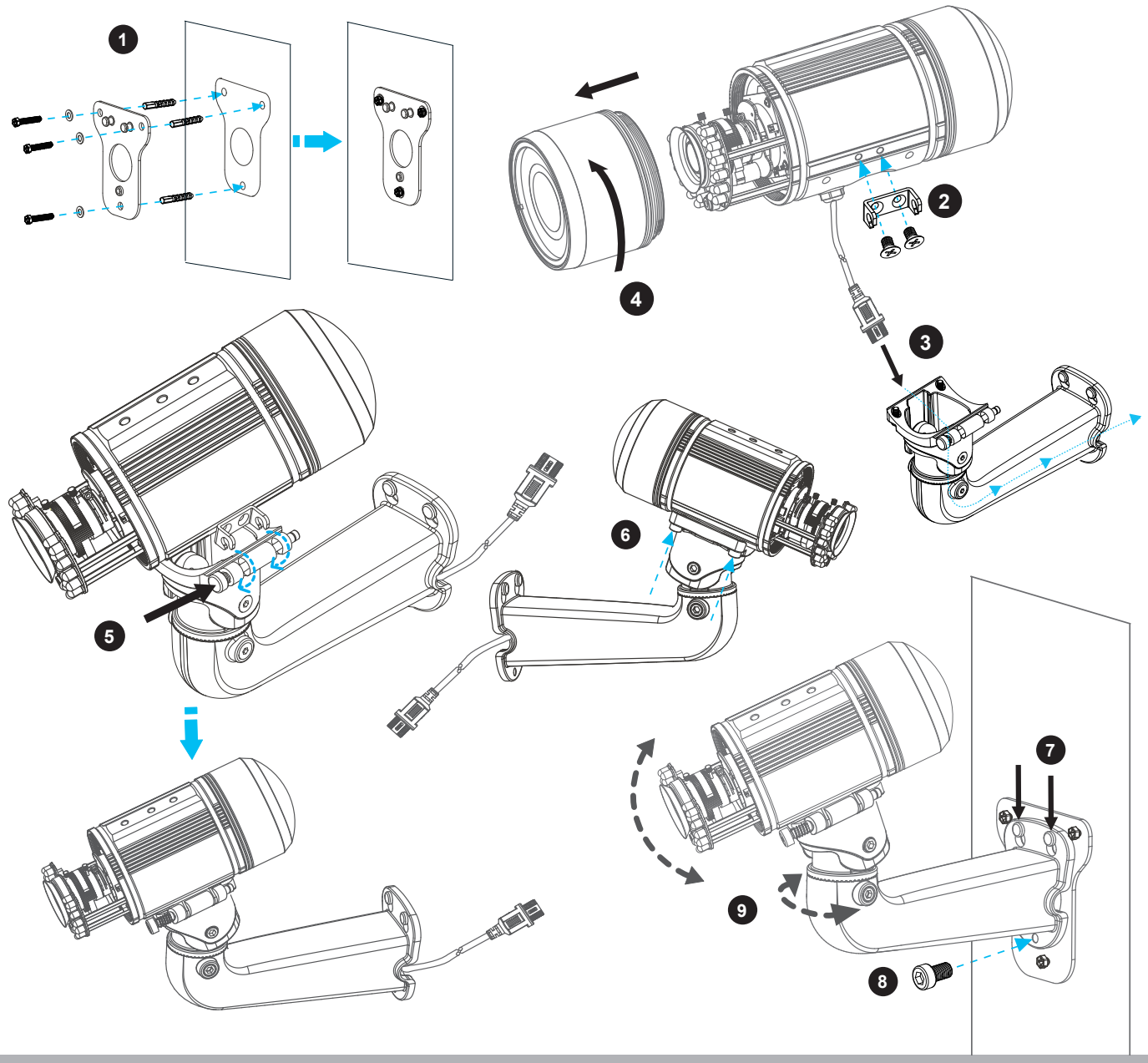


8. Connect the Ethernet cable to the RJ45 cable and secure the connectors tightly.



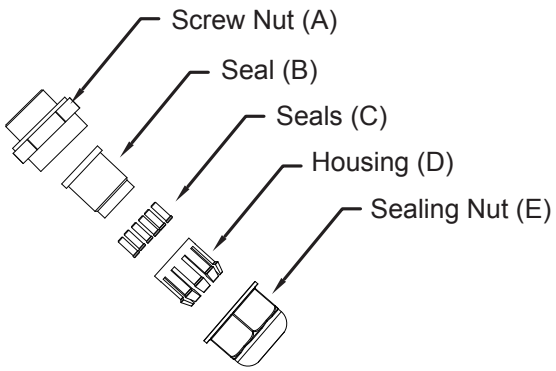
Hardware Installation

1. Attach the alignment sticker to the wall. Drill four holes into the wall. Then hammer the supplied plastic anchors into the holes and secure the plate with supplied screws.
2. Fix the ⊓-bracket to the side of the Network Camera with two screws.
3. Feed the RJ45 cable through the front opening of the wall mount bracket. (If you want to use external devices such as sensors and alarms, please refer to the assembling steps on the next page.)
4. Open the lens cover.
5. Push the spring mortise and hook the bracket onto the groove of the wall mount bracket.
6. Secure the two screws on the other side of the wall mount bracket.
7. Hang the wall mount bracket on the plate.
8. Fix the wall mount bracket with the supplied screw.
9. Adjust the angle of the wall mount bracket to aim at the shooting area.

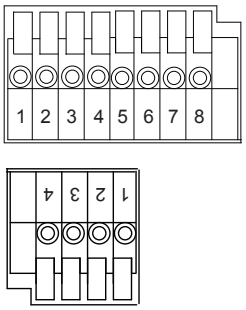


Waterproof Connector

Components of the Waterproof Connector



Pin Definition

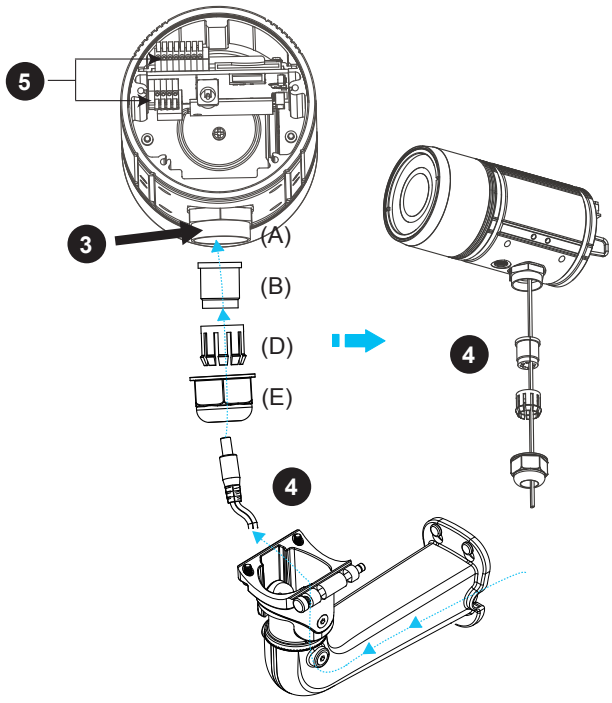


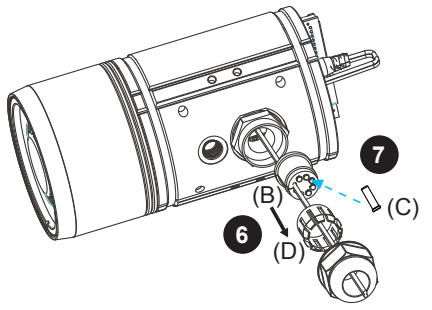
1	Power +12V
2	Digital Output
3	Digital Input
4	Ground
5	AC 24V
6	AC 24V
7	RS485 +
8	RS485 -

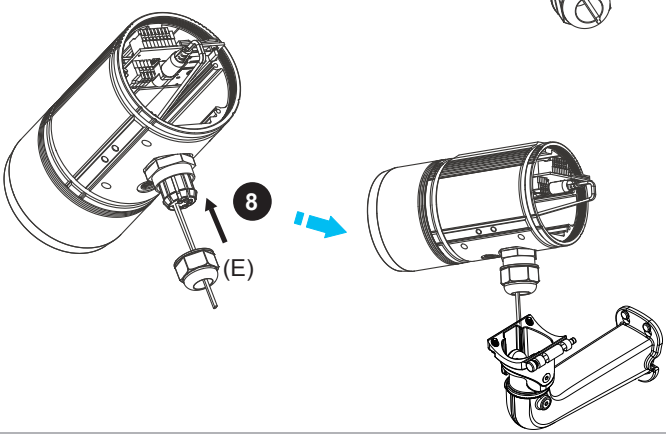
1	External MIC In
2	Ground
3	Audio Out
4	Ground

Assembling Steps

1. Disassemble the components of the waterproof connector into part (A) ~ (E) as shown above.
2. Open the back cover of the Network Camera.
3. Remove the rubber stopper from the bottom of the Network Camera and secure the screw nut (A) tightly.
4. If you need extra power for external devices, please feed the power cable through the wall mount bracket and the waterproof connector (E --> D --> B --> A) as the illustration shown below. Then connect the power cord to the socket. Note: There are 7 holes on the seal (B), and the widest hole with a crack on the side is specific for power cord.
5. If you have external devices such as sensors and alarms, feed the cables through the wall mount bracket and the waterproof connector (E --> D --> B --> A) as the illustration shown below. Then refer to the pin definition to connect them to the general I/O terminal block. Note: The recommended cable gauge is 2.0 ~ 2.8 mm.
6. Push the seal (B) into the housing (D).
7. Insert the seals (C) into the empty holes on the seal (B) to avoid moisture.
8. Secure the sealing nut (E) tightly.







Network Deployment

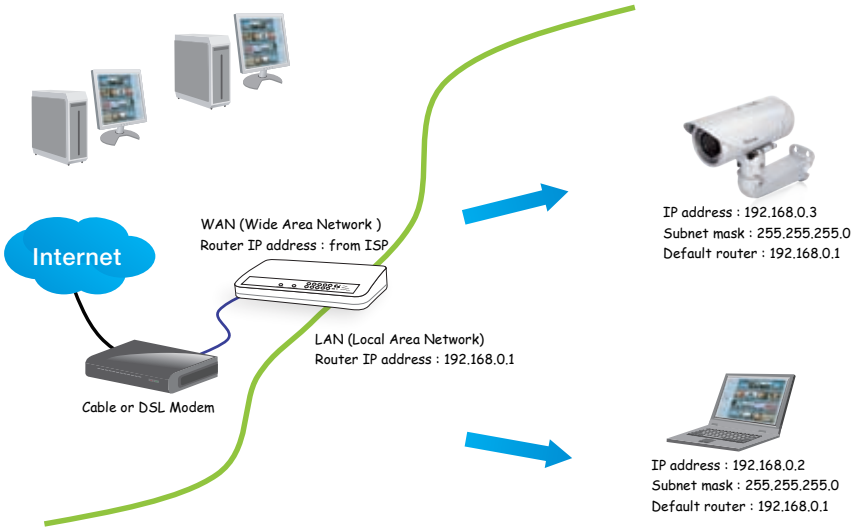
Setting up the Network Camera over the Internet

There are several ways to set up the Network Camera over the Internet. The first way is to set up the Network Camera behind a router. The second way is to utilize a static IP. The third way is to use PPPoE.

Internet connection via a router

Before setting up the Network Camera over the Internet, make sure you have a router and follow the steps below.

1. Connect your Network Camera behind a router, the Internet environment is illustrated below. Regarding how to obtain your IP address, please refer to Software Installation on page 13 for details.



2. In this case, if the Local Area Network (LAN) IP address of your Network Camera is 192.168.0.3, please forward the following ports for the Network Camera on the router.

- HTTP port
- RTSP port
- RTP port for audio
- RTCP port for audio
- RTP port for video
- RTCP port for video

If you have changed the port numbers on the Network page, please open the ports accordingly on your router. For information on how to forward ports on the router, please refer to your router's user's manual.

3. Find out the public IP address of your router provided by your ISP (Internet Service Provider). Use the public IP and the secondary HTTP port to access the Network Camera from the Internet. Please refer to Network Type on page 38 for details.

Internet connection with static IP

Choose this connection type if you are required to use a static IP for the Network Camera. Please refer to LAN on page 38 for details.

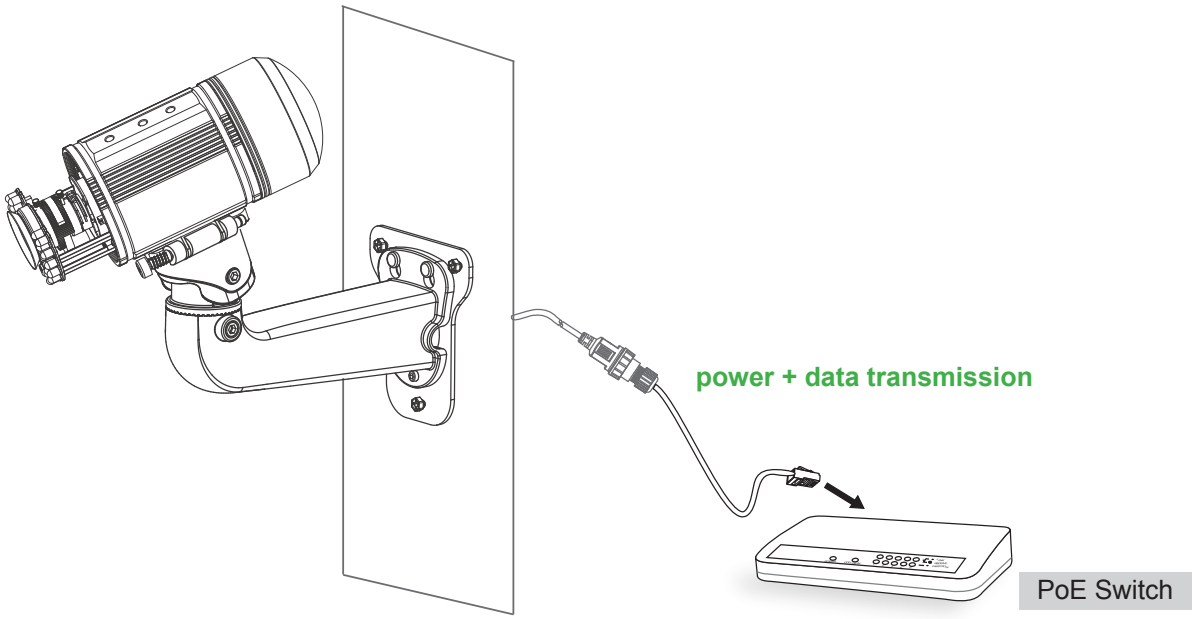
Internet connection via PPPoE (Point-to-Point over Ethernet)

Choose this connection type if you are connected to the Internet via a DSL Line. Please refer to PPPoE on page 39 for details.

Set up the Network Camera through Power over Ethernet (PoE)

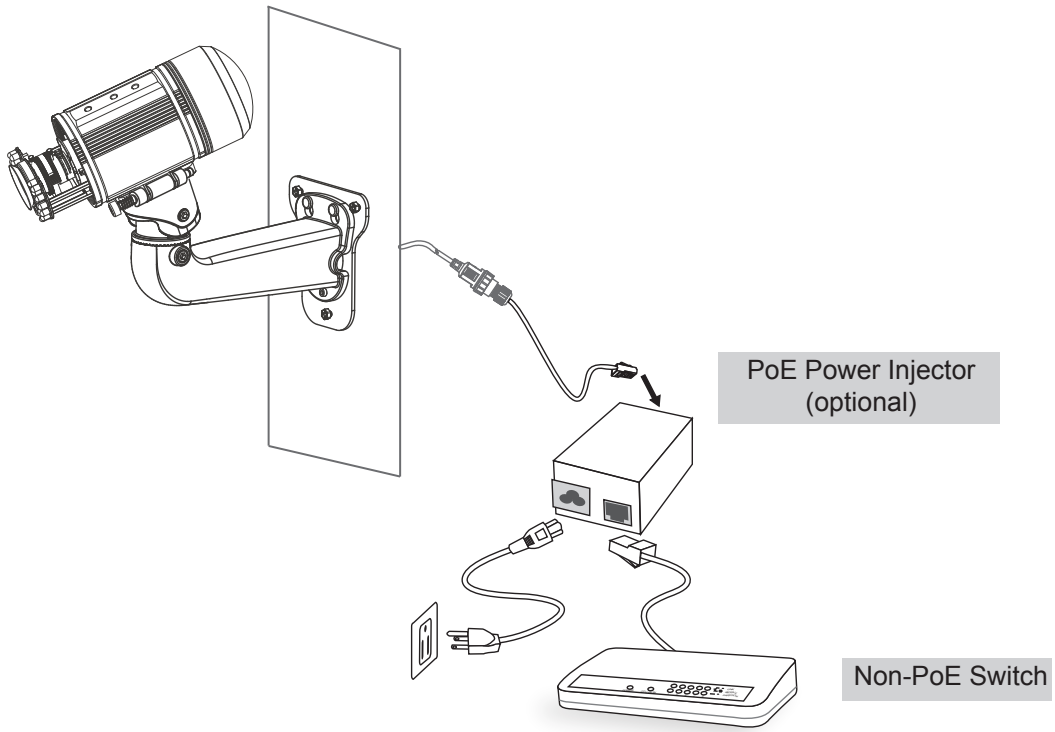
When using a PoE-enabled switch

The Network Camera is PoE-compliant, allowing transmission of power and data via a single Ethernet cable. Follow the below illustration to connect the Network Camera to a PoE-enabled switch via Ethernet cable.



When using a non-PoE switch

If your switch/router does not support PoE, use a PoE power injector (optional) to connect between the Network Camera and a non-PoE switch.



Software Installation

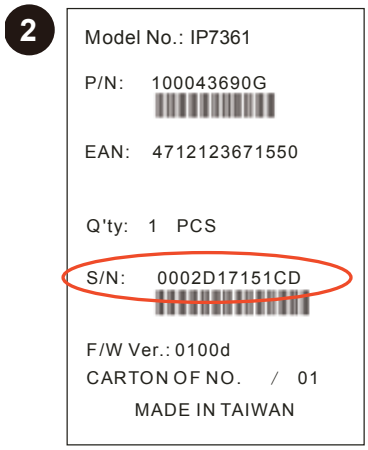
Installation Wizard 2 (IW2), free-bundled software included on the product CD, helps you set up your Network Camera on the LAN.

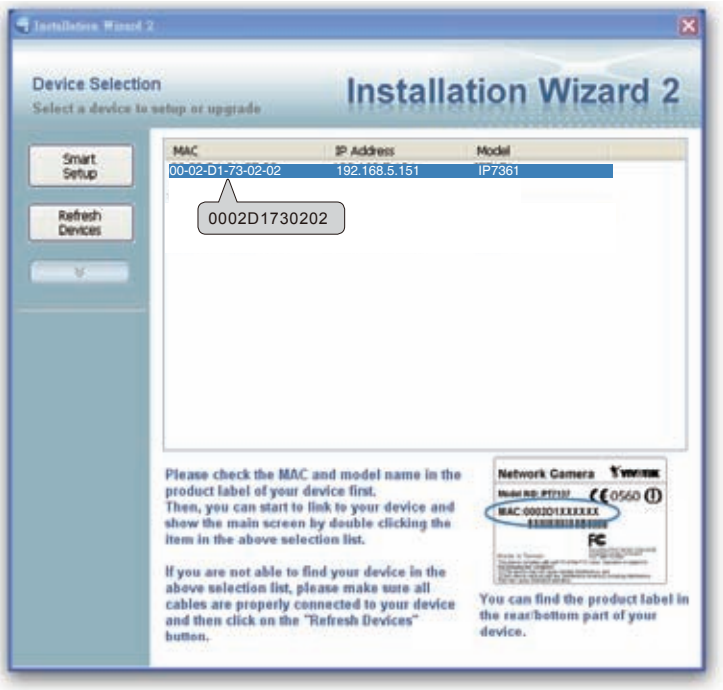
1. Install IW2 under the Software Utility directory from the software CD. Double click the IW2 shortcut on your desktop to launch the program.

2. The program will conduct an analysis of your network environment. After your network environment is analyzed, please click **Next** to continue the program.

3. The program will search for all VIVOTEK network devices on the same LAN.

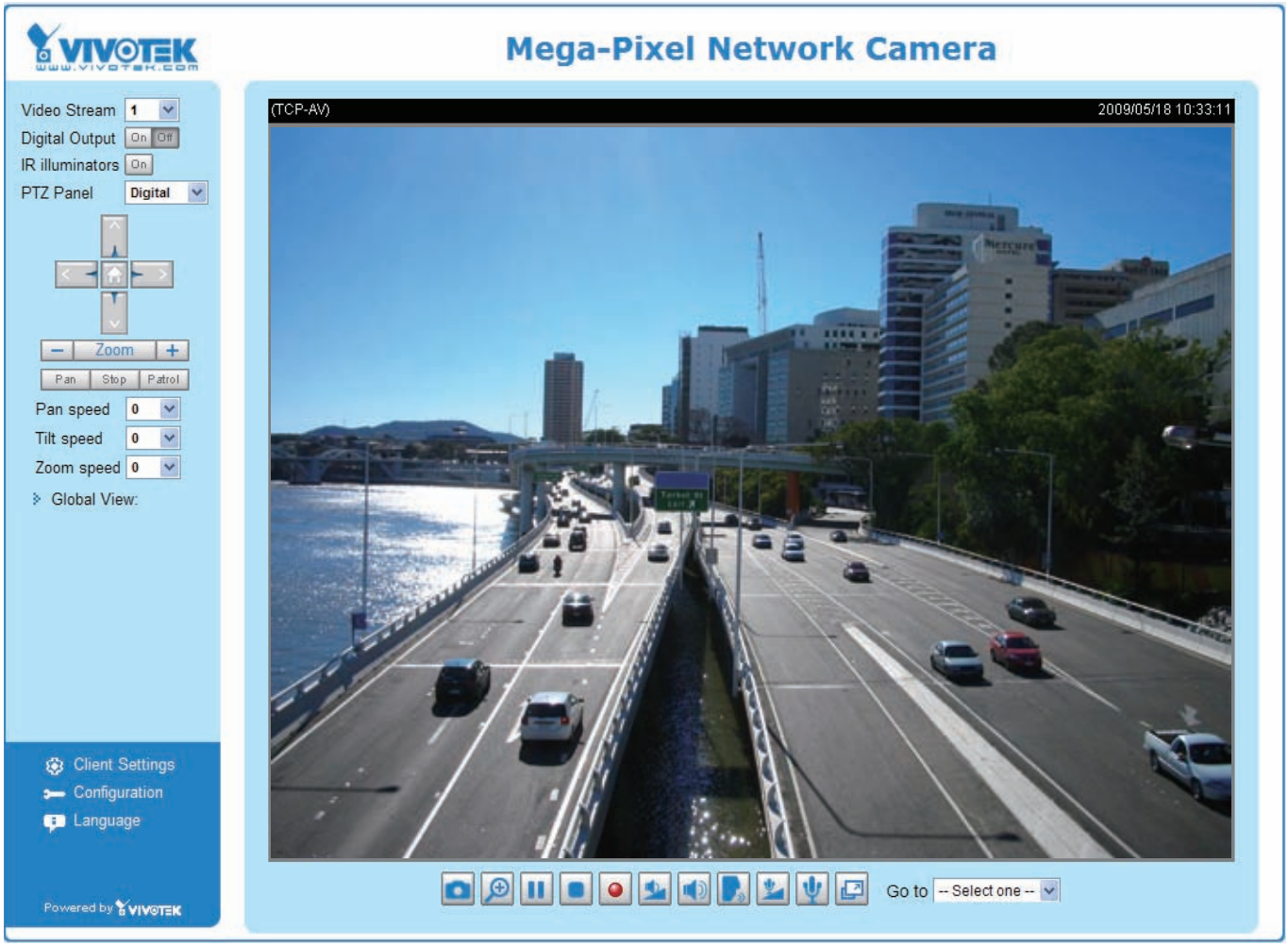
4. After searching, the main installer window will pop up. Click on the MAC and model name which matches the product label on your device to connect to the Network Camera via Internet Explorer.



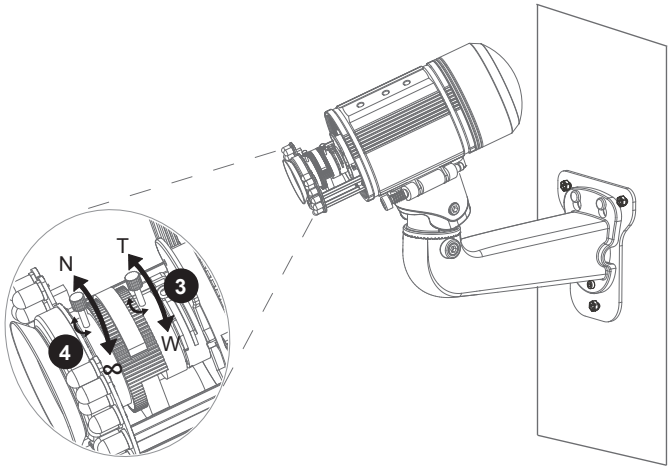


Ready to Use

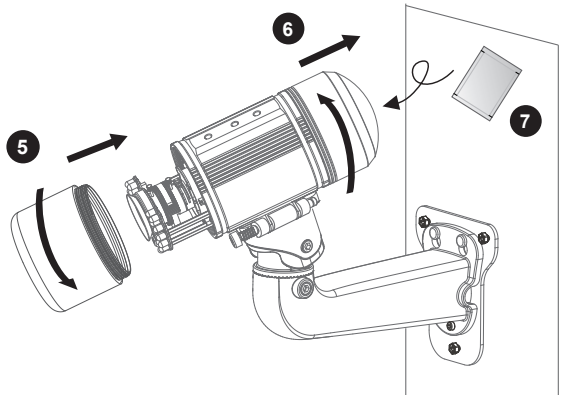
1. Access the Network Camera on the LAN.
2. Retrieve live video through a web browser or recording software.



3. Unscrew the zoom controller to adjust the zoom factor. Upon completion, tighten the zoom controller.
4. Unscrew the focus controller to adjust the focus range. Upon completion, tighten the focus controller.



5. Tighten the lens cover.
6. Open the back cover.
7. Tear down the aluminum foil vacuum bag and take out the silica gel. Attach the silica gel to the inner side of the back cover, then tighten the back cover. (Please replace the silica gel with a new one if you open the back cover after installation.)



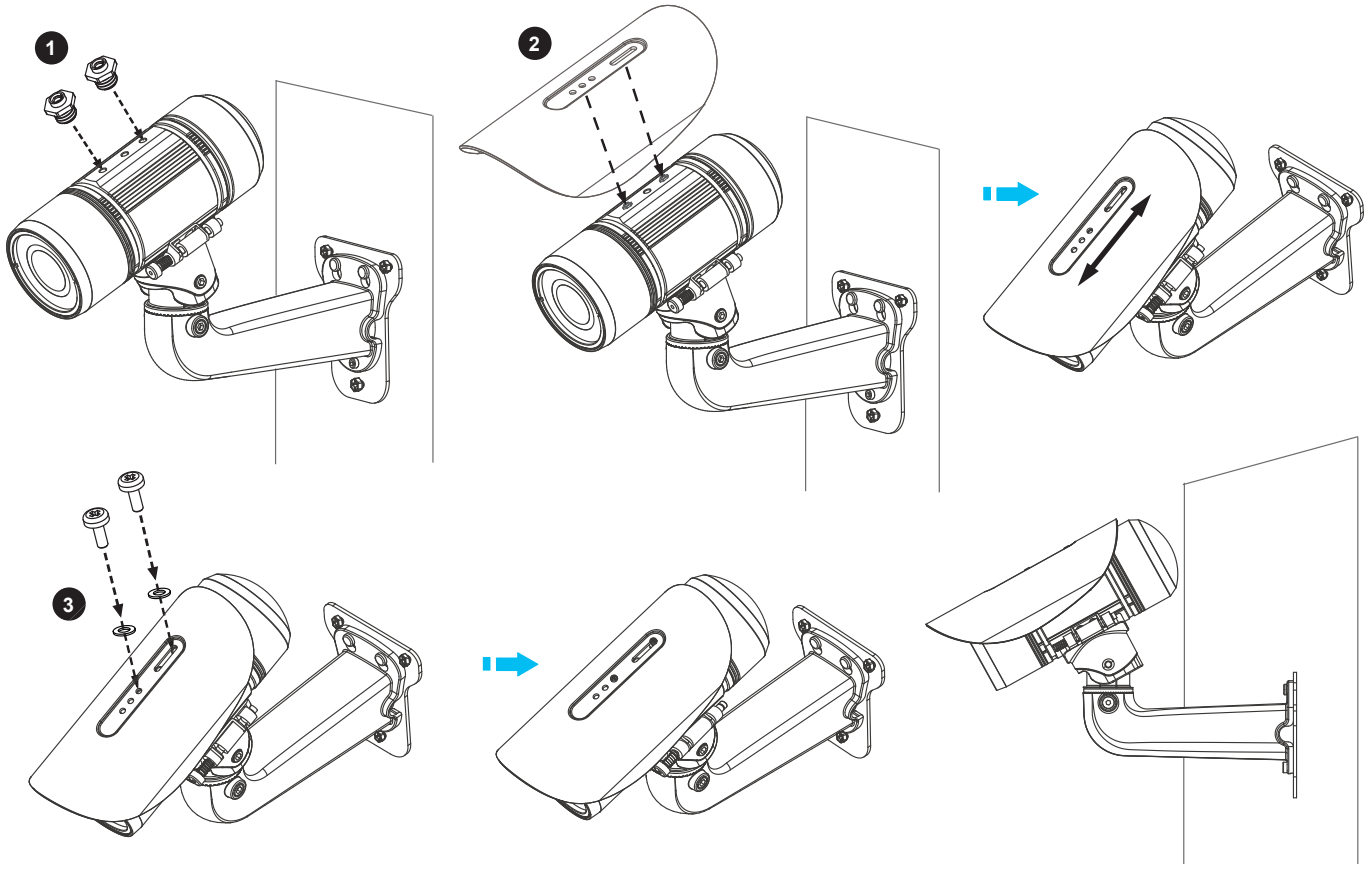
Note

If you want to use the supplied sun shield for outdoor environments, please follow the steps below to install:

1. Tighten the supplied two screws.

2. Attach the supplied sun shield to the Network Camera and slide it to the desired position.

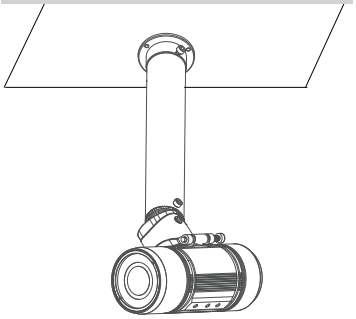
3. Fix the sun shield with the supplied two screws.



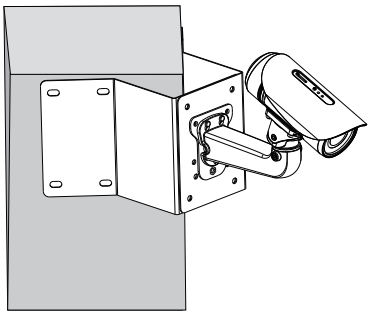
Accessories

VIVOTEK also provides other accessories for versatile applications as the following illustrations. Please visit VIVOTEK's official website for more purchase information.

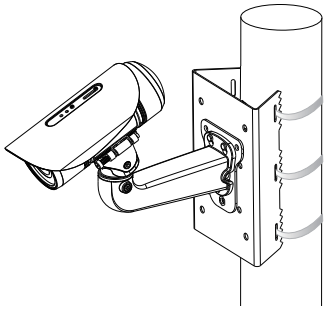
Pendant Mount Bracket



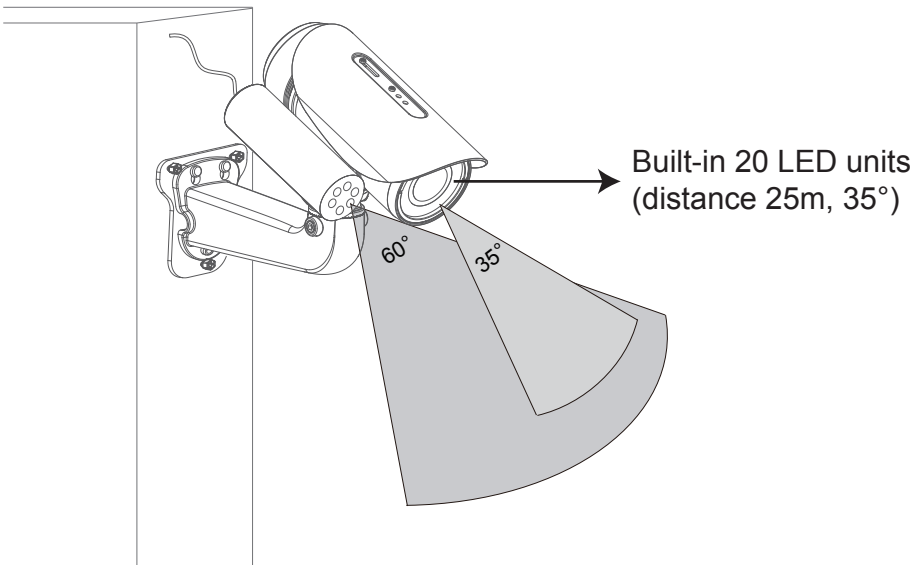
Corner Mount Bracket



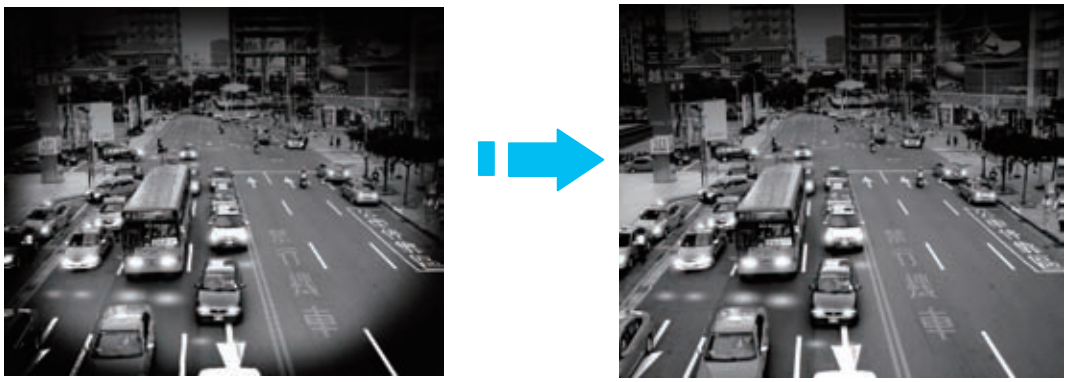
Pole Mount Bracket



IR illuminator (distance 30m, 60°)



The 30m, 60° IR illuminator extends the coverage of the Network Camera and reduces the halo effect around captured images.



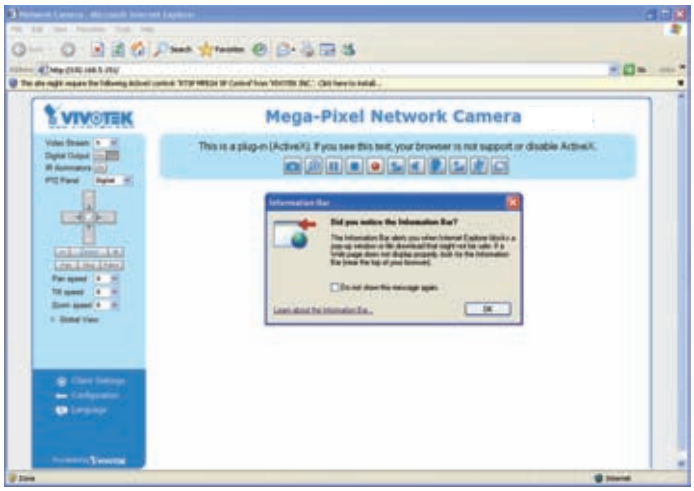
Accessing the Network Camera

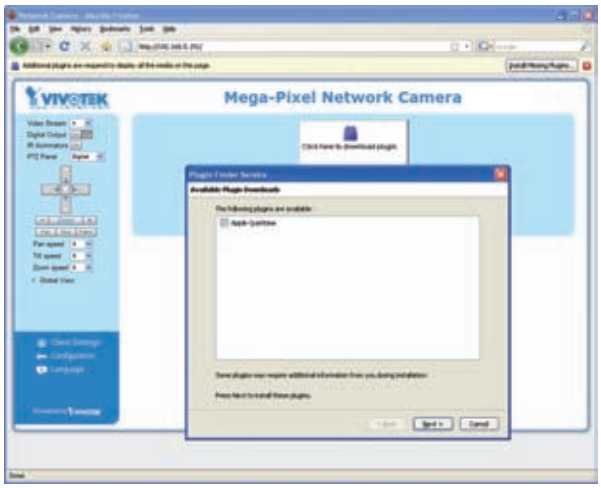
This chapter explains how to access the Network Camera through web browsers, RTSP players, 3GPP-compatible mobile devices, and VIVOTEK recording software.

Using Web Browsers

Use Installation Wizard 2 (IW2) to access to the Network Cameras on the LAN.
If your network environment is not a LAN, follow these steps to access the Netwotk Camera:

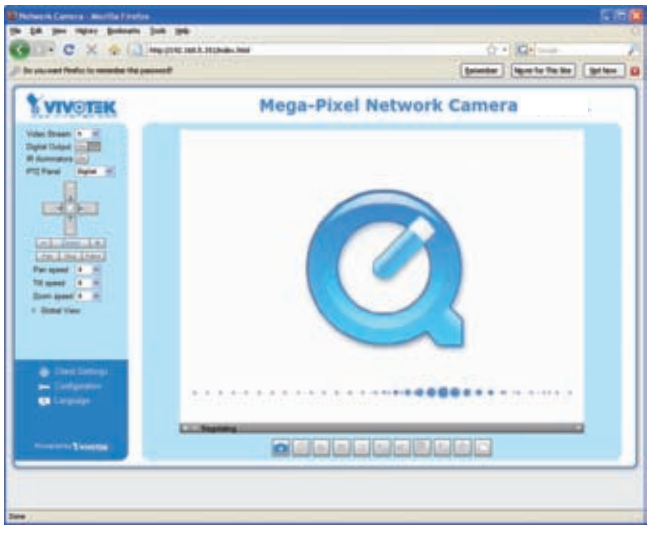
1. Launch your web browser (ex. Microsoft® Internet Explorer, Mozilla Firefox, or Netscape).
2. Enter the IP address of the Network Camera in the address field. Press **Enter**.
3. The live video will be displayed in your web browser.
4. If it is the first time installing the VIVOTEK network camera, an information bar will pop up as shown below. Follow the instructions to install the required plug-in on your computer.





NOTE

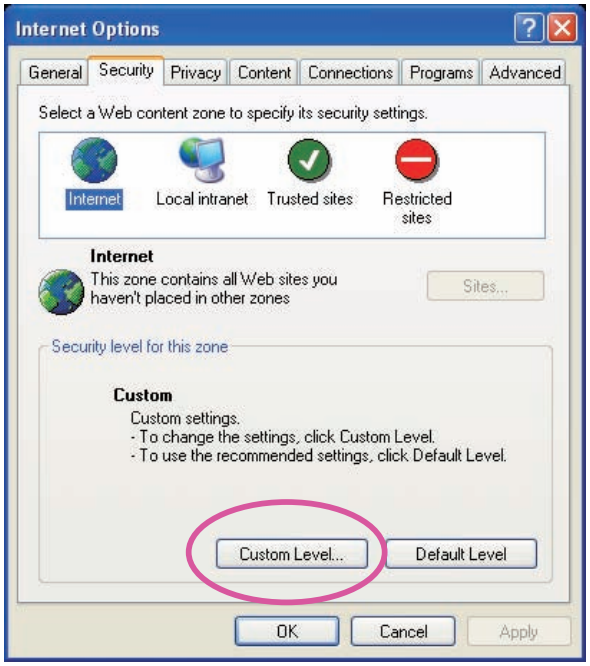
► *For Mozilla Firefox or Netscape users, your browser will use Quick Time to stream the live video. If you do not have Quick Time on your computer, please download it first, then launch the web browser.*



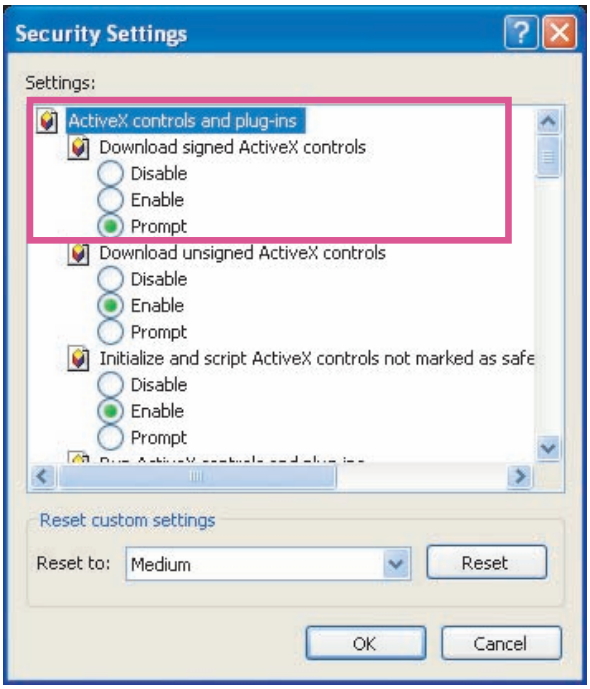
► *By default, the Network Camera is not password-protected. To prevent unauthorized access, it is highly recommended to set a password for the Network Camera.*
For more information about how to enable password protection, please refer to Security on page 31.

► *If you see a dialog box indicating that your security settings prohibit running ActiveX® Controls, please enable the ActiveX® Controls for your browser.*

1. Choose Tools > Internet Options > Security > Custom Level.



*2. Look for Download signed ActiveX® controls; select Enable or Prompt. Click **OK**.*



3. Refresh your web browser, then install the Active X® control. Follow the instructions to complete installation.

Using RTSP Players

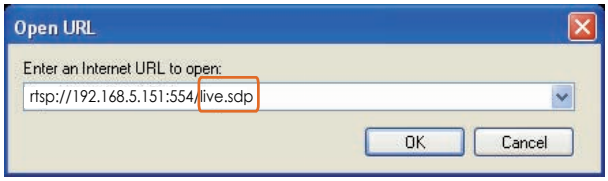
To view the MPEG-4 streaming media using RTSP players, you can use one of the following players that support RTSP streaming.

Quick Time Player

Real Player

1. Launch the RTSP player.
2. Choose File > Open URL. A URL dialog box will pop up.
3. The address format is rtsp://<ip address>:<rtsp port>/<RTSP streaming access name for stream1 or stream2>

As most ISPs and players only allow RTSP streaming through port number 554, please set the RTSP port to 554. For more information, please refer to RTSP Streaming on page 51.
For example:



4. The live video will be displayed in your player.
   For more information on how to configure the RTSP access name, please refer to RTSP Streaming on page 51 for details.

Using 3GPP-compatible Mobile Devices

To view the streaming media through 3GPP-compatible mobile devices, make sure the Network Camera can be accessed over the Internet. For more information on how to set up the Network Camera over the Internet, please refer to Setup the Network Camera over the Internet on page 10.

To utilize this feature, please check the following settings on your Network Camera:

1. Because most players on 3GPP mobile phones do not support RTSP authentication, make sure the authentication mode of RTSP streaming is set to disable.
   For more information, please refer to RTSP Streaming on page 51.

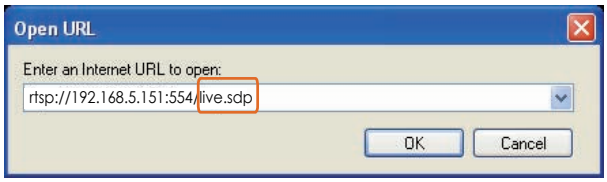
2. As the the bandwidth on 3G networks is limited, you will not be able to use a large video size. Please set the video and audio streaming parameters as listed below.
   For more information, please refer to Viewing Window on page 64.

Video Mode	MPEG-4
Frame size	176 x 144
Maximum frame rate	5 fps
Intra frame period	1S
Video quality (Constant bit rate)	40kbps
Audio type (GSM-AMR)	12.2kbps

3. As most ISPs and players only allow RTSP streaming through port number 554, please set the RTSP port to 554. For more information, please refer to RTSP Streaming on page 51.

4. Launch the player on the 3GPP-compatible mobile devices (ex. Real Player).

5. Type the following URL commands into the player.
   The address format is rtsp://<public ip address of your camera>:<rtsp port>/<RTSP streaming access name for stream 3>.
   For example:

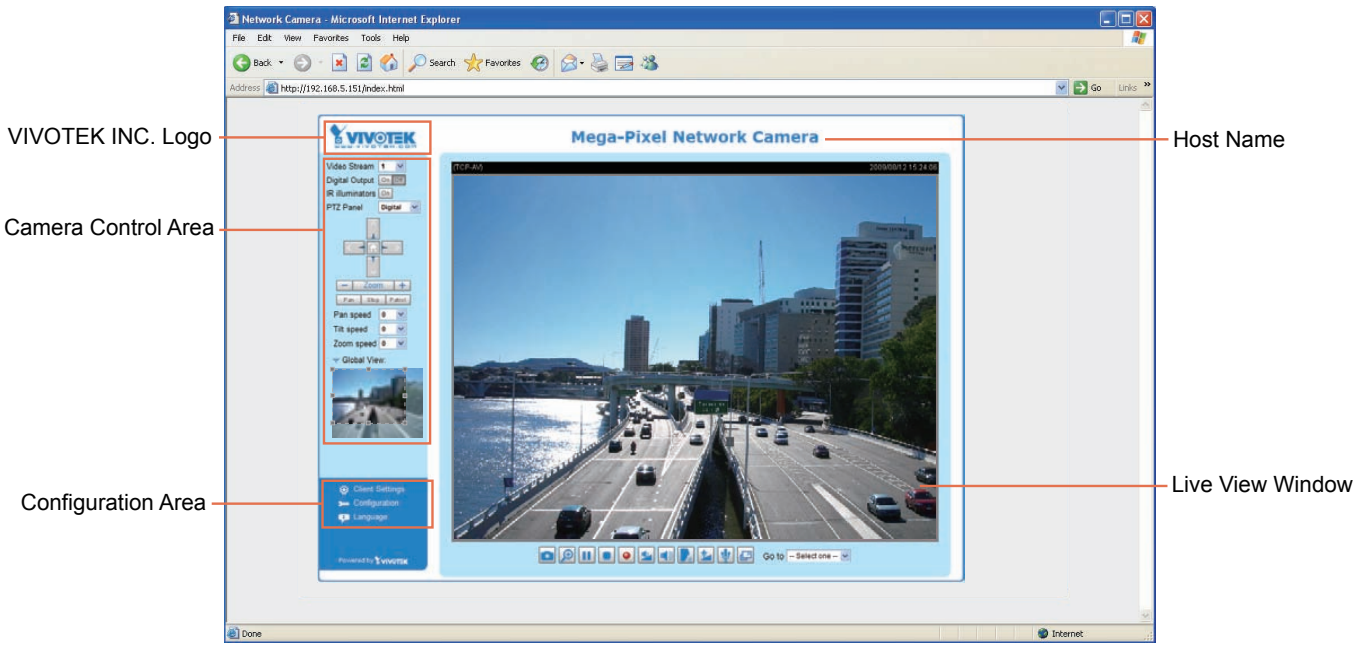


Using VIVOTEK Recording Software

The product software CD also contains recording software, allowing simultaneous monitoring and video recording for multiple Network Cameras. Please install the recording software; then launch the program to add the Network Camera to the Channel list. For detailed information about how to use the recording software, please refer to the user's manual of the software or download it from http://www.vivotek.com.

Main Page

This chapter explains the layout of the main page. It is composed of the following sections: VIVOTEK INC. Logo, Host Name, Camera Control Area, Configuration Area, Menu, and Live Video Window.



VIVOTEK INC. Logo

Click this logo to visit the VIVOTEK website.

Host Name

The host name can be customized to fit your needs. For more information, please refer to System on page 29.

Camera Control Area

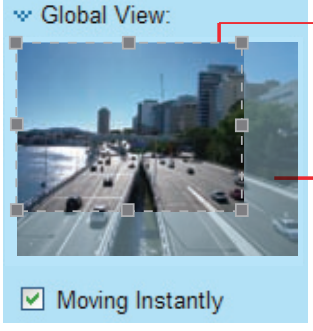
Video Stream: This Network Cmera supports multiple streams (stream 1 ~ 4) simultaneously. You can select either one for live viewing. For more information about multiple streams, please refer to page 64 for detailed information.

Digital Output: Click to turn the digital output device on or off.

IR Illuminators: Click to turn on the IR LEDs for 20 seconds.

PTZ Panel: This Network Camera supports both “digital“ (e-PTZ) and “mechanical“ pan/tilt/zoom control. Please refer to Camera Control on page 75 for detailed information.

Global View: Click on this item to display the Global View window. The Global View window contains a full view image (the largest frame size of the captured video) and a floating frame (the viewing region of the curruent video stream). The floating frame allows users to control the e-PTZ function (Electronic Pan/Tilt/Zoom). For more information about e-PTZ operation, please refer to E-PTZ Operation on page 80. For more information about how to set up the viewing region of the current video stream, please refer to Viewing Windows on page 64.



Configuration Area

Client Settings: Click this button to access the client setting page. For more information, please refer to Client Settings on page 26.

Configuration: Click this button to access the configuration page of the Network Camera. It is suggested that a password be applied to the Network Camera so that only the administrator can configure the Network Camera. For more information, please refer to Configuration on page 28.

Language: Click this button to choose a language for the user interface. Language options are available in: English, Deutsch, Español, Français, Italiano, 日本語, Português, 簡体中文, and 繁體中文.

Live Video Window

■ The following window is displayed when the video mode is set to MPEG-4:

Video Title: The video title can be configured. For more information, please refer to Video Settings on page 58.

MPEG-4 Protocol and Media Options: The transmission protocol and media options for MPEG-4 video streaming. For further configuration, please refer to Client Settings on page 26.

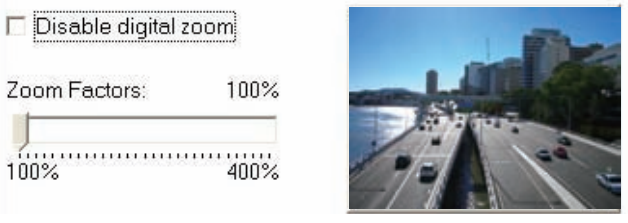
Time: Display the current time. For further configuration, please refer to Video Settings on page 58.

Title and Time: The video title and time can be stamped on the streaming video. For further configuration, please refer to Video Settings on page 58.

Video and Audio Control Buttons: Depending on the Network Camera model and Network Camera configuration, some buttons may not be available.

Snapshot: Click this button to capture and save still images. The captured images will be displayed in a pop-up window. Right-click the image and choose **Save Picture As** to save it in JPEG (*.jpg) or BMP (*.bmp) format.

Digital Zoom: Click and uncheck “Disable digital zoom” to enable the zoom operation. The navigation screen indicates the part of the image being magnified. To control the zoom level, drag the slider bar. To move to a different area you want to magnify, drag the navigation screen.



Pause: Pause the transmission of the streaming media. The button becomes the Resume button after clicking the Pause button.

Stop: Stop the transmission of the streaming media. Click the Resume button to continue transmission.

Start MP4 Recording: Click this button to record video clips in MP4 file format to your computer. Press the Stop MP4 Recording button to end recording. When you exit the web browser, video recording stops accordingly. To specify the storage destination and file name, please refer to MP4 Saving Options on page 27 for details.

Volume: When the Mute function is not activated, move the slider bar to adjust the volume on the local computer.

Mute: Turn off the volume on the local computer. The button becomes the Audio On button after clicking the Mute button.

Talk: Click this button to talk to people around the Network Camera. Audio will project from the external speaker connected to the Network Camera. Click this button again to end talking transmission.

Mic Volume: When the Mute function is not activated, move the slider bar to adjust the microphone volume on the local computer.

Mute: Turn off the Mic volume on the local computer. The button becomes the Mic On button after clicking the Mute button.

Full Screen: Click this button to switch to full screen mode. Press the “Esc” key to switch back to normal mode.

■ The following window is displayed when the video mode is set to MJPEG:

Video Title: The video title can be configured. For more information, please refer to Video Settings on page 58.

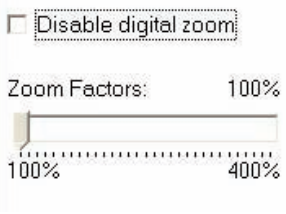
Time: Display the current time. For more information, please refer to Video Settings on page 58.

Title and Time: Video title and time can be stamped on the streaming video. For more information, please refer to Video Settings on page 58.

Video and Audio Control Buttons: Depending on the Network Camera model and Network Camera configuration, some buttons may not be available.

Snapshot: Click this button to capture and save still images. The captured images will be displayed in a pop-up window. Right-click the image and choose **Save Picture As** to save it in JPEG (*.jpg) or BMP (*.bmp) format.

Digital Zoom: Click and uncheck “Disable digital zoom” to enable the zoom operation. The navigation screen indicates the part of the image being magnified. To control the zoom level, drag the slider bar. To move to a different area you want to magnify, drag the navigation screen.



Start MP4 Recording: Click this button to record video clips in MP4 file format to your computer. Press the Stop MP4 Recording button to end recording. When you exit the web browser, video recording stops accordingly. To specify the storage destination and file name, please refer to MP4 Saving Options on page 27 for details.

Full Screen: Click this button to switch to full screen mode. Press the “Esc” key to switch back to normal mode.

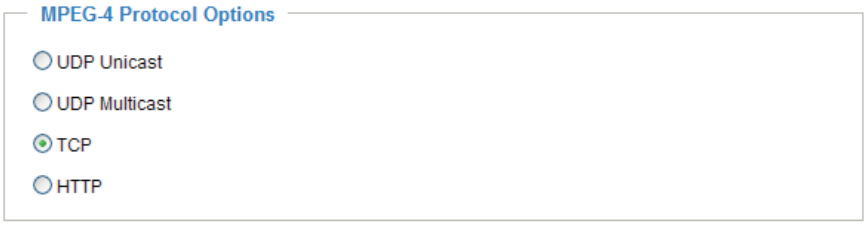
Client Settings

This chapter explains how to select the stream transmission mode and saving options on the local computer. When completed with the settings on this page, click **Save** on the page bottom to enable the settings.

MPEG-4 Media Options

Select to stream video or audio data or both. This is enabled only when the video mode is set to MPEG-4.

MPEG-4 Protocol Options



Depending on your network environment, there are four transmission modes of MPEG-4 streaming:

UDP unicast: This protocol allows for more real-time audio and video streams. However, network packets may be lost due to network burst traffic and images may be broken. Activate UDP connection when occasions require time-sensitive responses and the video quality is less important. Note that each unicast client connecting to the server takes up additional bandwidth and the Network Camera allows up to ten simultaneous accesses.

UDP multicast: This protocol allows multicast-enabled routers to forward network packets to all clients requesting streaming media. This helps to reduce the network transmission load of the Network Camera while serving multiple clients at the same time. Note that to utilize this feature, the Network Camera must be configured to enable multicast streaming at the same time. For more information, please refer to RTSP Streaming on page 51.

TCP: This protocol guarantees the complete delivery of streaming data and thus provides better video quality. The downside of this protocol is that its real-time effect is not as good as that of the UDP protocol.

HTTP: This protocol allows the same quality as TCP protocol without needing to open specific ports for streaming under some network environments. Users inside a firewall can utilize this protocol to allow streaming data through.

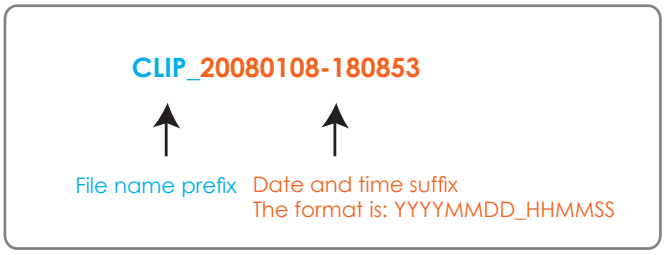
MP4 Saving Options

Users can record live video as they are watching it by clicking Start MP4 Recording on the main page. Here, you can specify the storage destination and file name.

Folder: Specify a storage destination for the recorded video files.

File name prefix: Enter the text that will be appended to the front of the video file name.

Add date and time suffix to the file name: Select this option to append the date and time to the end of the file name.



Configuration

Click **Configuration** on the main page to enter the camera setting pages. Note that only Administrators can access the configuration page.

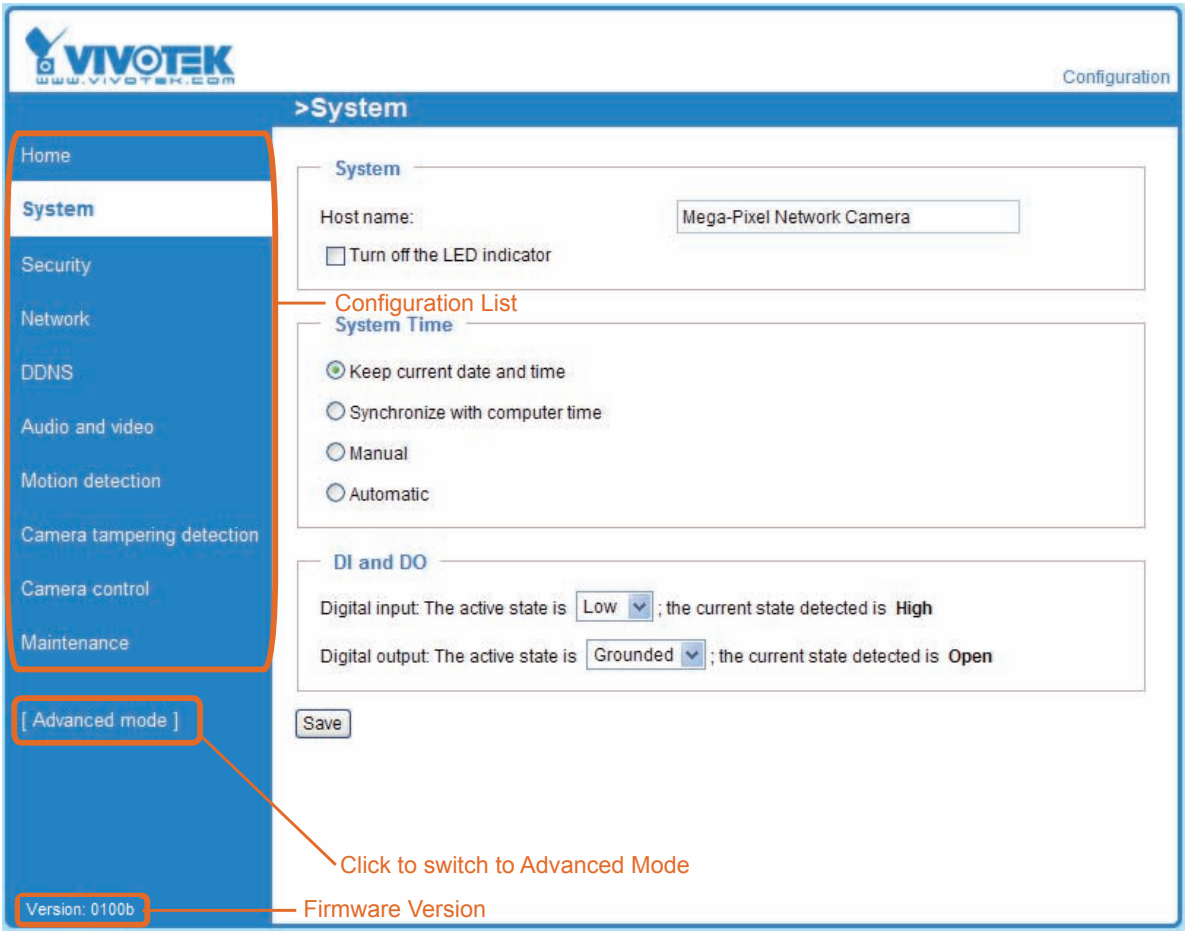
VIVOTEK offers an easy-to-use user interface that helps you set up your network camera with minimal effort. To simplify the setting procedure, two types of user interfaces are available: Advanced Mode for professional users and Basic Mode for entry-level users. Some advanced functions (HTTPS/ Access list/ Homepage layout/ Application/ Recording/ System log/ View parameters) are not displayed in Basic Mode.

If you want to set up advanced functions, please click **[Advanced Mode]** on the bottom of the configuration list to quickly switch to Advanced Mode.

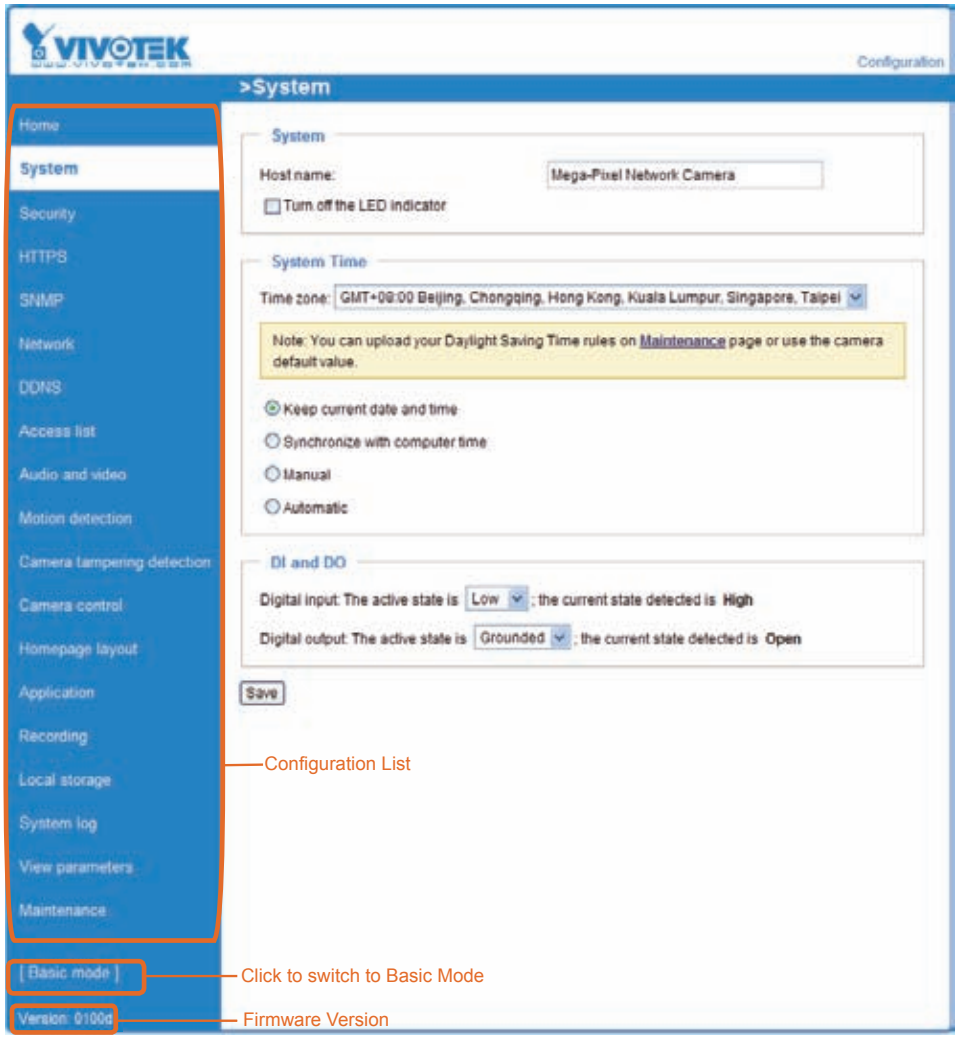
In order to simplify the user interface, the detailed information will be hidden unless you click on the function item. When you click on the first sub-item, the detailed information for the first sub-item will be displayed; when you click on the second sub-item, the detailed information for the second sub-item will be displayed and that of the first sub-item will be hidden.

The following is the interface of the Basic Mode and the Advanced Mode:

Basic Mode



Advanced Mode



Each function on the configuration list will be explained in the following sections. Those functions that are displayed only in Advanced Mode are marked with Advanced Mode. If you want to set up advanced functions, please click **[Advanced Mode]** on the bottom of the configuration list to quickly switch over.

System

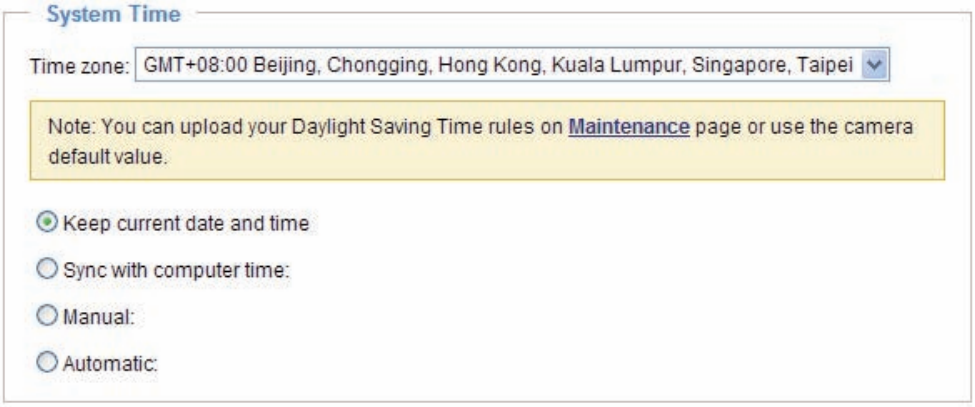
This section explains how to configure the basic settings for the Network Camera, such as the host name and system time. It is composed of the following three columns: System, System Time and DI and DO. When finished with the settings on this page, click **Save** at the bottom of the page to enable the settings.

System

Host name: Enter a desired name for the Network Camera. The text will be displayed at the top of the main page.

Turn off the LED indicators: If you do not want to let others know that the network camera is in operation, you can select this option to turn off the LED indicators.

System Time



Keep current date and time: Select this option to preserve the current date and time of the Network Camera. The Network Camera's internal real-time clock maintains the date and time even when the power of the system is turned off.

Sync with computer time: Select this option to synchronize the date and time of the Network Camera with the local computer. The read-only date and time of the PC is displayed as updated.

Manual: The administrator can enter the date and time manually. Note that the date and time format are [yyyy/mm/dd] and [hh:mm:ss].

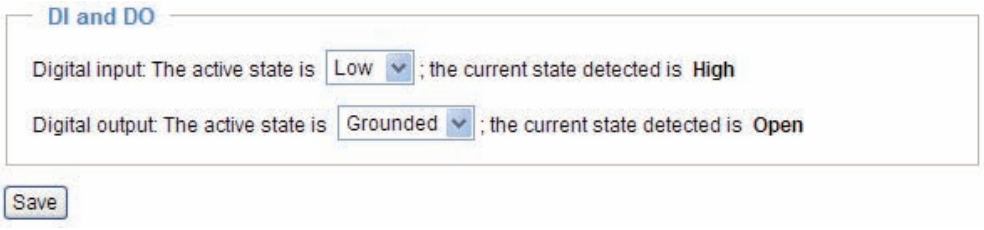
Automatic: The Network Time Protocol is a protocol which synchronizes computer clocks by periodically querying an NTP Server.

NTP server: Assign the IP address or domain name of the time-server. Leaving the text box blank connects the Network Camera to the default time servers.

Update interval: Select to update the time using the NTP server on an hourly, daily, weekly, or monthly basis.

Time zone Advanced Mode: Select the appropriate time zone from the list. If you want to upload Daylight Savings Time rules on the Maintenance page, please refer to Upload / Export Daylight Saving Time Configuration File on page 108 for details.

DI and DO



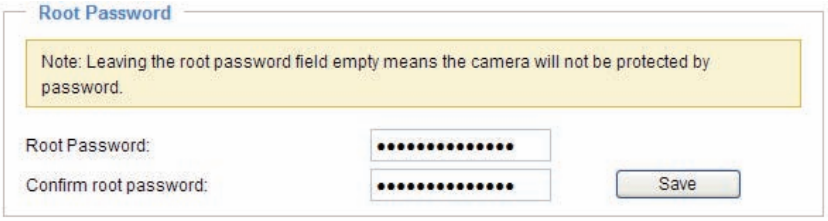
Digital input: Select High or Low to define normal status for the digital input. The Network Camera will report the current status.

Digital output: Select Grounded or Open to define normal status for the digital output. The Network Camera will show whether the trigger is activated or not.

Security

This section explains how to enable password protection and create multiple accounts.

Root Password



The administrator account name is “root”, which is permanent and can not be deleted. If you want to add more accounts in the Manage User column, please apply the password for the “root” account first.

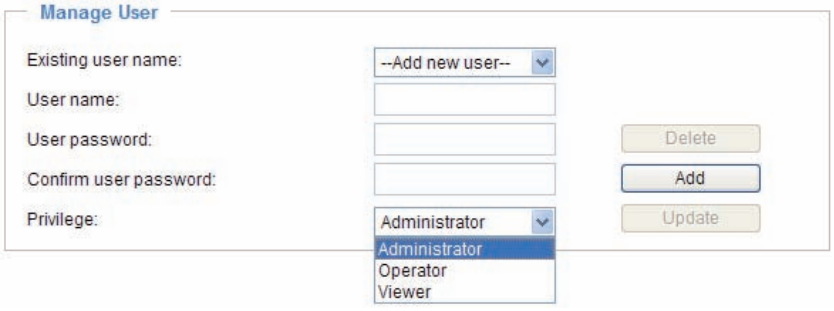
1. Type the password identically in both text boxes, then click **Save** to enable password protection.
2. A window will be prompted for authentication; type the correct user’s name and password in their respective fields to access the Network Camera.

Manage Privilege Advanced Mode

Digital Output & IR illuminators: You can modify the manage privilege of operators or viewers. Check or uncheck the item, then click **Save** to enable the settings. If you give Viewers the privilege, Operators will also have the ability to control the Network Camera through the main page. (Please refer to Main Page on page 22.)

Allow anonymous viewing: If you check this item, any client can access the live stream without entering a User ID and Password.

Manage User



Administrators can add up to 20 user accounts.

1. Input the new user’s name and password.
2. Select the privilege level for the new user account. Click **Add** to enable the setting.

Access rights are sorted by user privilege (Administrator, Operator, and Viewer). Only administrators can access the Configuration page. Though operators cannot access the Configuration page, they can use the URL Commands to get and set the value of parameters. For more information, please refer to URL Commands of the Network Camera on page 111. Viewers access only the main page for live viewing.

Here you also can change a user’s access rights or delete user accounts.

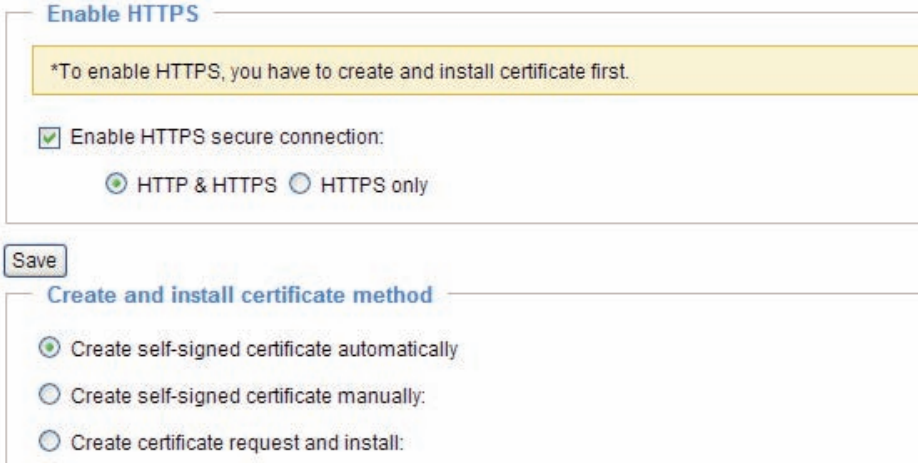
1. Select an existing account to modify.
2. Make necessary changes and click **Update** or **Delete** to enable the setting.

HTTPS (Hypertext Transfer Protocol over SSL) Advanced Mode

This section explains how to enable authentication and encrypted communication over SSL (Secure Socket Layer). It helps protect streaming data transmission over the Internet on higher security level.

Enable HTTPS

Check this item to enable HTTPS communication, then select a connection option: "HTTP & HTTPS" or "HTTPS only". Note that you have to create and install a certificate first in the second column before clicking the **Save** button.

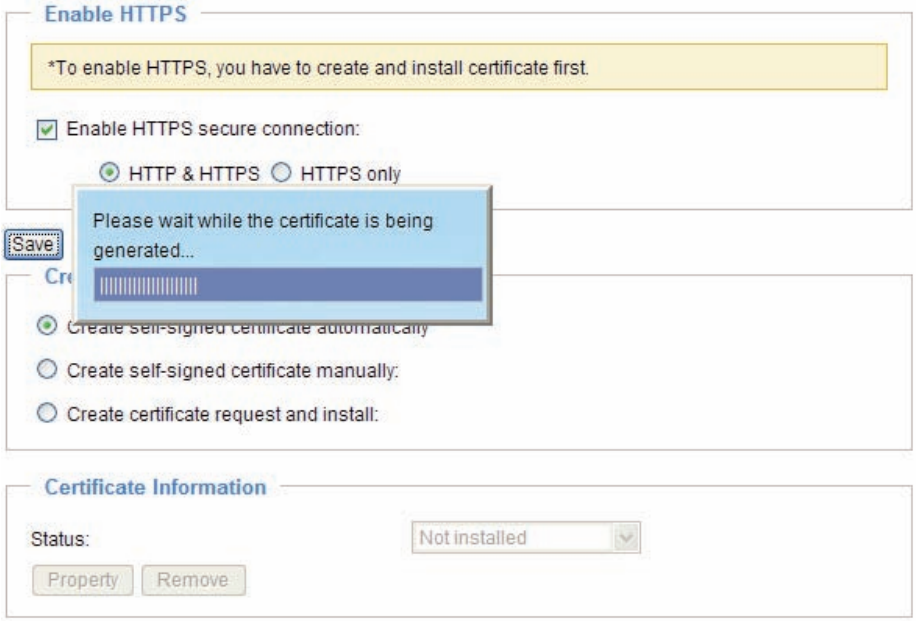


Create and Install Certificate Method

Before using HTTPS for communication with the Network Camera, a **Certificate** must be created first. There are three ways to create and install a certificate:

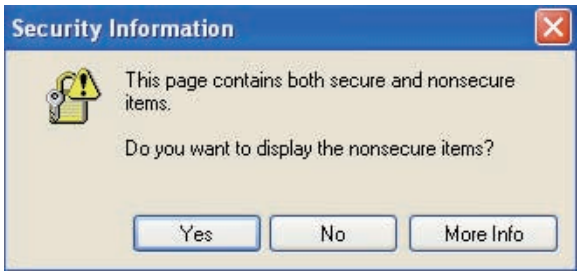
Create self-signed certificate automatically

1. Select this option.
2. In the first column, check **Enable HTTPS secure connection**, then select a connection option: “HTTP & HTTPS” or “HTTPS only”.
3. Click **Save** to generate a certificate.



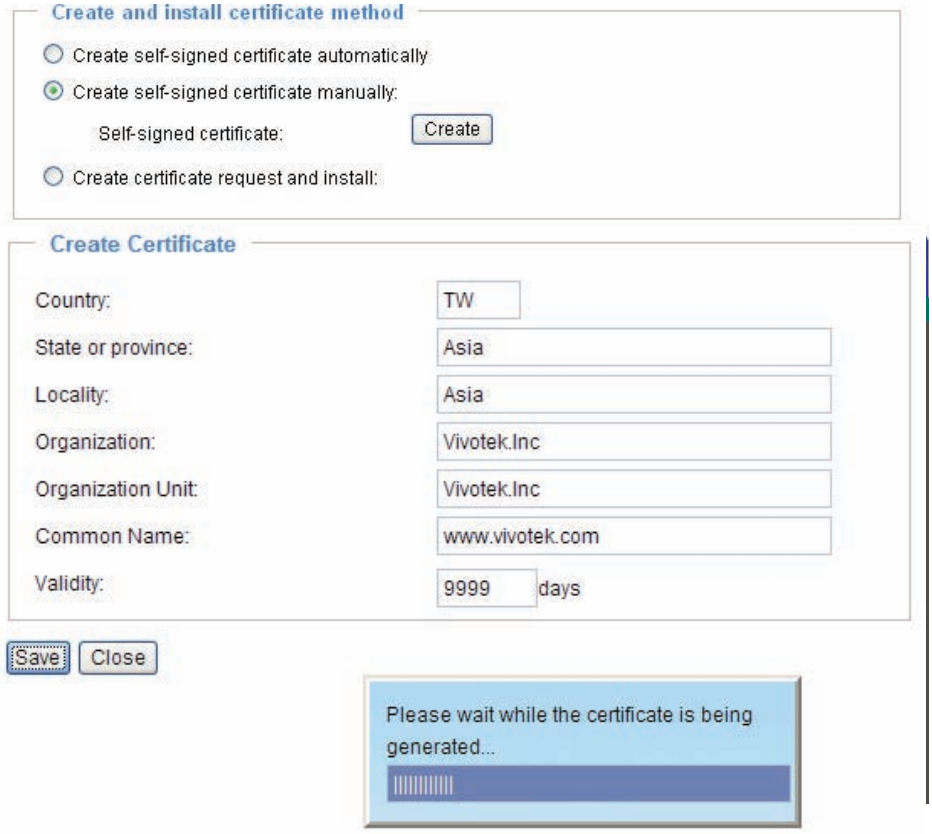
4. The Certificate Information will automatically de displayed in the third column as shown below. You can click **Property** to view detailed information about the certificate.

5. Click **Home** to return to the main page. Change the address from "http://" to "https://" in the address bar and press **Enter** on your keyboard. Some Security Alert dialogs will pop up. Click **OK** or **Yes** to enable HTTPS.



Create self-signed certificate manually

1. Select this option.
2. Click **Create** to open the Create Certificate page, then click **Save** to generate the certificate.

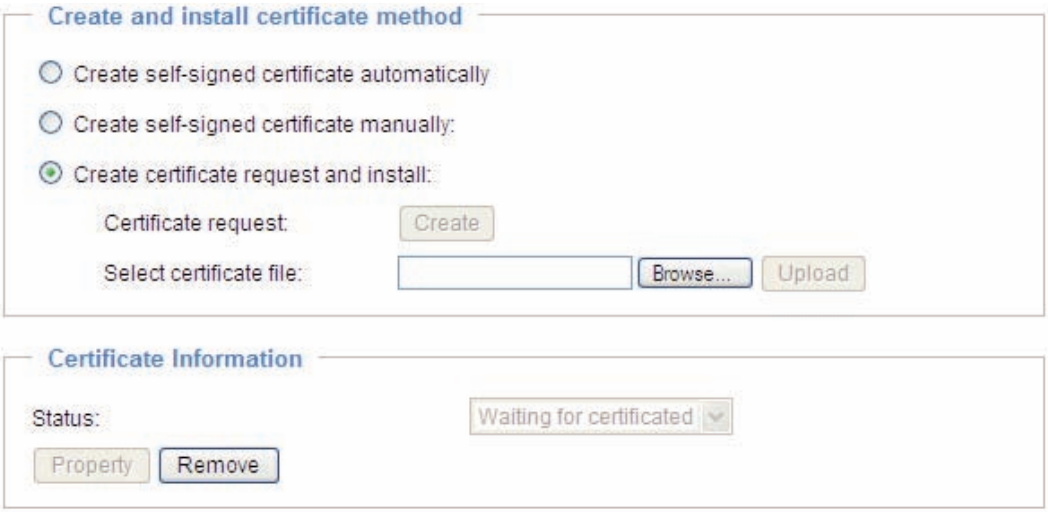


3. The Certificate Information will automatically be displayed in the third column as shown below. You can click **Property** to see detailed information about the certificate.

Create certificate and install : Select this option if you want to create a certificate from a certificate authority.

1. Select this option.
2. Click **Create** to open the Create Certificate page, then click **Save** to generate the certificate.

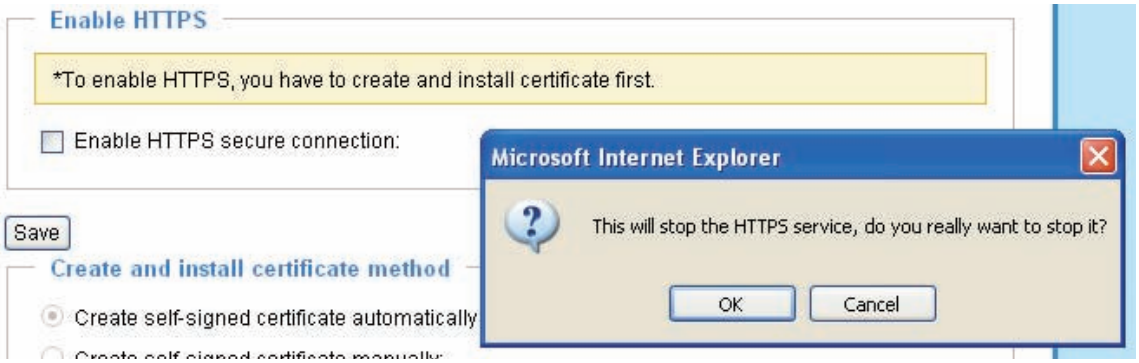
5. Look for a trusted certificate authority that issues digital certificates. Enroll the Network Camera. Wait for the certificate authority to issue a SSL certificate; click **Browse...** to search for the issued certificate, then click Upload in the second column.



NOTE

► *How do I cancel the HTTPS settings?*

1. *Uncheck **Enable HTTPS secure connection** in the first column and click **Save**; a warning dialog will pop up.*
2. *Click **OK** to disable HTTPS.*



3. *The webpage will redirect to a non-HTTPS page automatically.*

► *If you want to create and install other certificates, please remove the existing one. To remove the signed certificate, uncheck **Enable HTTPS secure connection** in the first column and click **Save**. Then click **Remove** to erase the certificate.*

SNMP (Simple Network Management Protocol) Advanced Mode

This section explains how to use the SNMP on the network camera. The Simple Network Management Protocol is an application layer protocol that facilitates the exchange of management information between network devices. It helps network administrators to remotely manage network devices and find, solve network problems with ease.

■ The SNMP consists of the following three key components:
1. Manager: Network-management station (NMS), a server which executes applications that monitor and control managed devices.
2. Agent: A network-management software module on a managed device which transfers the status of managed devices to the NMS.
3. Managed device: A network node on a managed network. For example: routers, switches, bridges, hubs, computer hosts, printers, IP telephones, network cameras, web server, and database.

Before configuring SNMP settings on the this page, please enable your NMS first.

SNMP Configuration

Enable SNMPv1, SNMPv2c
Select this option and enter the names of Read/Write community and Read Only community according to your NMS settings.

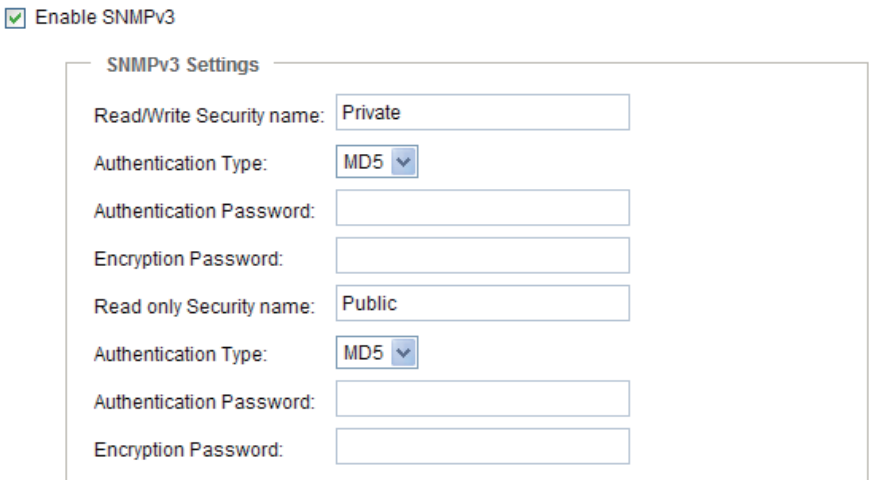
Enable SNMPv3
This option contains cryptographic security, a higher security level, which allows you to set the Authentication password and the Encryption password.

■ Security name: According to your NMS settings, choose Read/Write or Read Only and enter the community name.

■ Authentication type: Select MD5 or SHA as the authentication method.

■ Authentication password: Enter the password for authenrication (at least 8 characters).

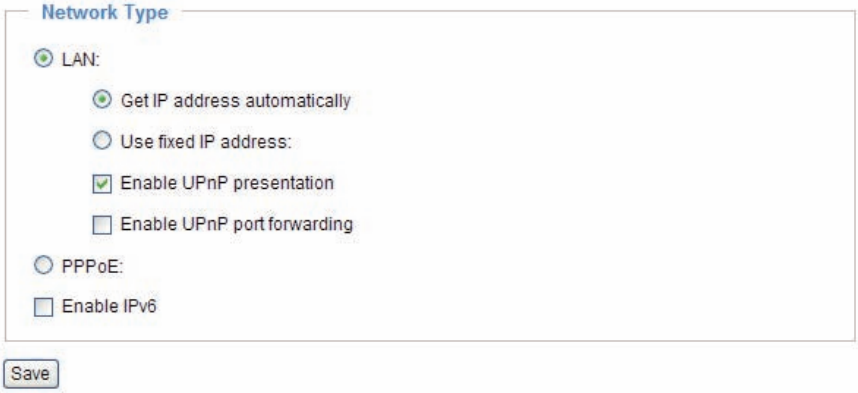
■ Encryption password: Enter a password for ecryption (at least 8 characters).



Network

This section explains how to configure a wired network connection for the Network Camera.

Network Type

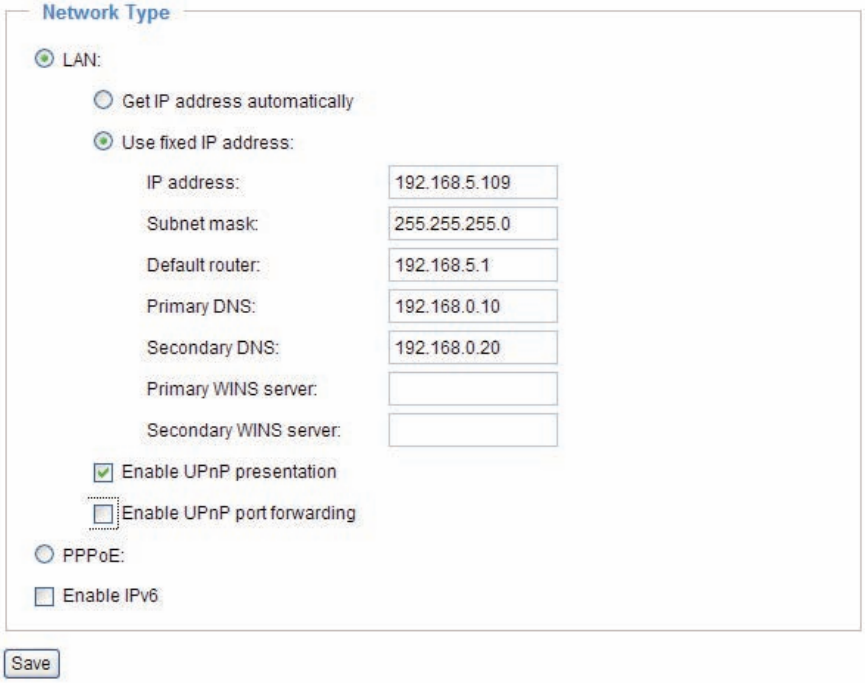


LAN

Select this option when the Network Camera is deployed on a local area network (LAN) and is intended to be accessed by local computers. The default setting for the Network Type is LAN. Rememer to click **Save** when you complete the Network setting.

Get IP address automatically: Select this option to obtain an available dynamic IP address assigned by the DHCP server each time the camera is connected to the LAN.

Use fixed IP address: Select this option to manually assign a static IP address to the Network Camera.



1. You can make use of VIVOTEK Installation Wizard 2 on the software CD to easily set up the Network Camera on LAN. Please refer to Software Installation on page 13 for details.
2. Enter the Static IP, Subnet mask, Default router, and Primary DNS provided by your ISP.

Subnet mask: This is used to determine if the destination is in the same subnet. The default value is “255.255.255.0”.

Default router: This is the gateway used to forward frames to destinations in a different subnet. Invalid router setting will fail the transmission to destinations in different subnet.

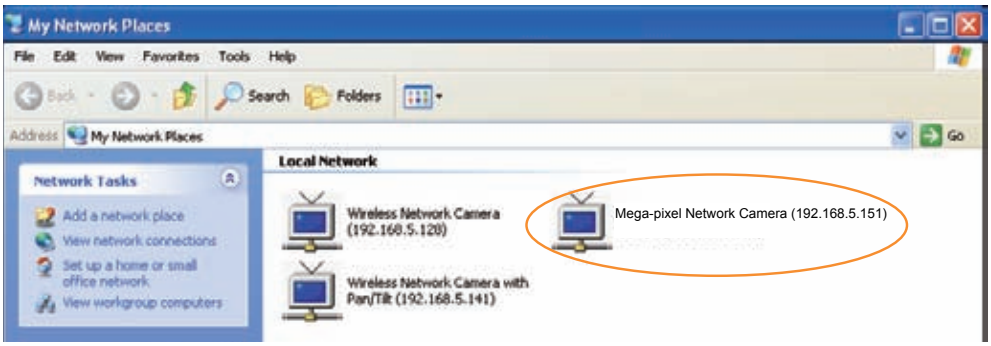
Primary DNS: The primary domain name server that translates hostnames into IP addresses.

Secondary DNS: Secondary domain name server that backups the Primary DNS.

Primary WINS server: The primary WINS server that maintains the database of computer name and IP address.

Secondary WINS server: The secondary WINS server that maintains the database of computer name and IP address.

Enable UPnP presentation: Select this option to enable UPnP™ presentation for your Network Camera so that whenever a Network Camera is presented to the LAN, shortcuts of connected Network Cameras will be listed in My Network Places. You can click the shortcut to link to the web browser. Currently, UPnP™ is supported by Windows XP or later. Note that to utilize this feature, please make sure the UPnP™ component is installed on your computer.



Enable UPnP port forwarding: To access the Network Camera from the Internet, select this option to allow the Network Camera to open ports on the router automatically so that video streams can be sent out from a LAN. To utilize of this feature, make sure that your router supports UPnP™ and it is activated.

PPPoE (Point-to-point over Ethernet)

Select this option to configure your Network Camera to make it accessible from anywhere as long as there is an Internet connection. Note that to utilize this feature, it requires an account provided by your ISP.

Follow the steps below to acquire your Network Camera's public IP address.

1. Set up the Network Camera on the LAN.
2. Go to Home > Configuration > Application > Server Settings (please refer to Server Settings on page 91) to add a new email or FTP server.
3. Go to Configuration > Application > Media Settings (please refer to Media Settings on page 94). Select System log so that you will receive the system log in TXT file format which contains the Network Camera's public IP address in your email or on the FTP server.
4. Go to Configuration > Network > Network Type. Select PPPoE and enter the user name and password provided by your ISP. Click **Save** to enable the setting.

5. The Network Camera will reboot.
6. Disconnect the power to the Network Camera; remove it from the LAN environment.

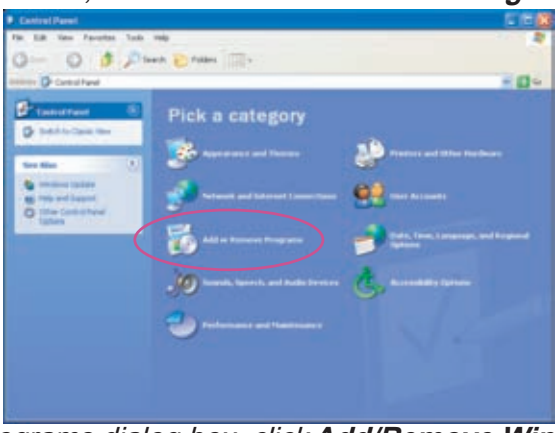
NOTE

► *If the default ports are already used by other devices connected to the same router, the Network Camera will select other ports for the Network Camera.*

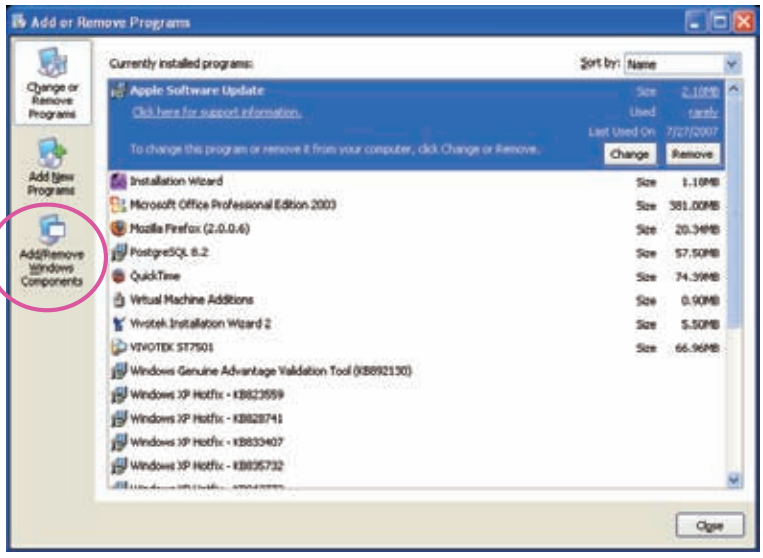
► *If UPnP™ is not supported by your router, you will see the following message:*
Error: Router does not support UPnP port forwarding.

► *Steps to enable the UPnP™ user interface on your computer:*
Note that you must log on to the computer as a system administrator to install the UPnP™ components.

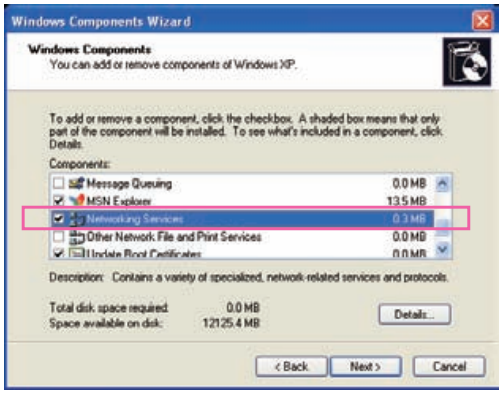
*1. Go to Start, click **Control Panel**, then click **Add or Remove Programs**.*



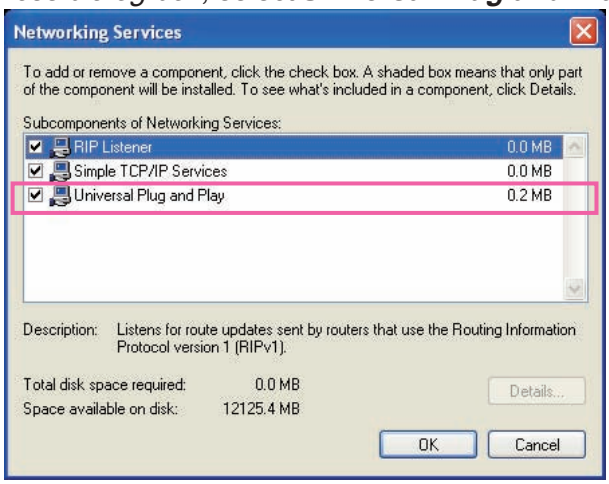
*2. In the Add or Remove Programs dialog box, click **Add/Remove Windows Components**.*



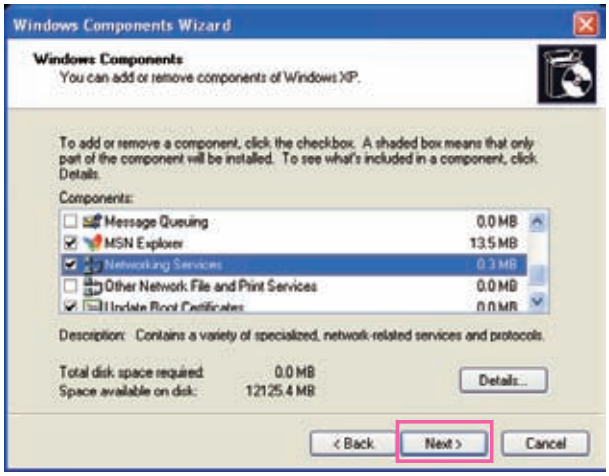
*3. In the Windows Components Wizard dialog box, select **Networking Services** and click **Details**.*



4. In the Networking Services dialog box, select ***Universal Plug and Play*** and click ***OK***.



5. Click ***Next*** in the following window.



6. Click ***Finish***. *UPnP™ is enabled.*

► *How does UPnP™ work?*
UPnP™ networking technology provides automatic IP configuration and dynamic discovery of devices added to a network. Services and capabilities offered by networked devices, such as printing and file sharing, are available among each other without the need for cumbersome network configuration. In the case of Network Cameras, you will see Network Camera shortcuts under My Network Places.

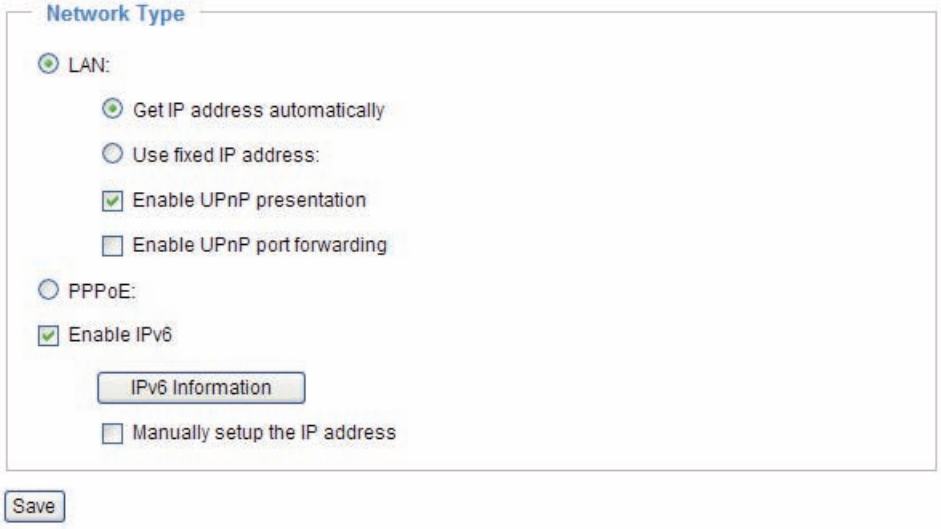
► *Enabling UPnP port forwarding allows the Network Camera to open a secondary HTTP port on the router-not HTTP port-meaning that you have to add the secondary HTTP port number to the Network Camera's public address in order to access the Network Camera from the Internet. For example, when the HTTP port is set to 80 and the secondary HTTP port is set to 8080, refer to the list below for the Network Camera's IP address.*

From the Internet	In LAN
http://203.67.124.123:8080	http://192.168.4.160 or http://192.168.4.160:8080

► *If the PPPoE settings are incorrectly configured or the Internet access is not working, restore the Network Camera to factory default; please refer to Restore on page 107 for details. After the Network Camera is reset to factory default, it will be accessible on the LAN.*

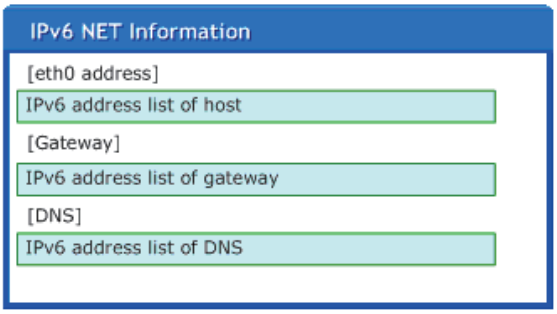
Enable IPv6

Select this option and click **Save** to enable IPv6 settings.
Please note that this only works if your network environment and hardware equipment support IPv6. The browser should be Microsoft® Internet Explorer 6.5, Mozilla Firefox 3.0 or above.

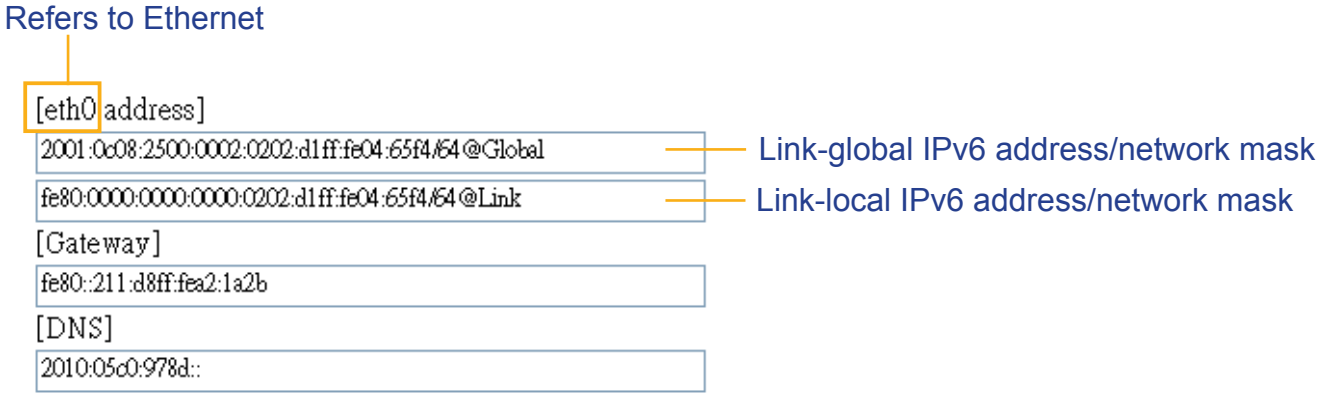


When IPv6 is enabled, by default, the network camera will listen to router advertisements and be assigned with a link-local IPv6 address accordingly.

IPv6 Information: Click this button to obtain the IPv6 information as shown below.

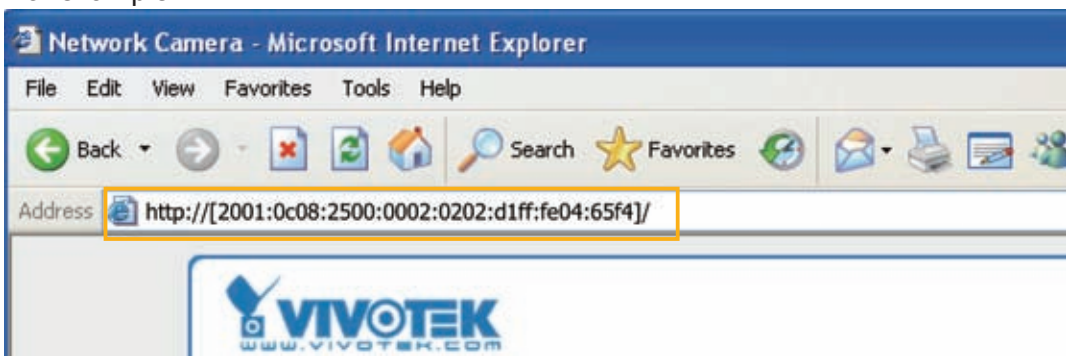


If your IPv6 settings are successful, the IPv6 address list will be listed in the pop-up window. The IPv6 address will be displayed as follows:



Please follow the steps below to link to an IPv6 address:
1. Open your web browser.
2. Enter the link-global or link-local IPv6 address in the address bar of your web browser.
3. The format should be:

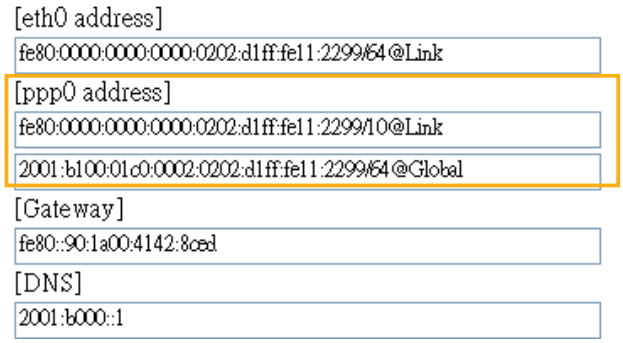
4. Press **Enter** on the keyboard or click **Refresh** button to refresh the webpage.
   For example:



NOTE

► *If you have a Secondary HTTP port (the default value is 8080), you can also link to the webpage in the following address format: (Please refer to **HTTP** on page 48 for detailed information.)*

► *If you choose PPPoE as the Network Type, the [PPP0 address] will be displayed in the IPv6 information column as shown below.*



Manually setup the IP address: Select this option to manually set up IPv6 settings if your network environment does not have DHCPv6 server and router advertisements-enabled routers.
If you check this item, the following blanks will be displayed for you to enter the corresponding information:

IEEE 802.1x Advanced Mode

Enable this function if your network environment uses IEEE 802.1x, which is a port-based network access control. The network devices, intermediary switch/access point/hub, and RADIUS server must support and enable 802.1x settings.

The 802.1x standard is designed to enhance the security of local area networks, which provides authentication to network devices (clients) attached to a network port (wired or wireless). If all certificates between client and server are verified, a point-to-point connection will be enabled; if authentication fails, access on that port will be prohibited. 802.1x utilizes an existing protocol, the Extensible Authentication Protocol (EAP), to facilitate communication.

■ The components of a protected network with 802.1x authentication:

Supplicant
(Network Camera)

Authenticator
(Network Switch)

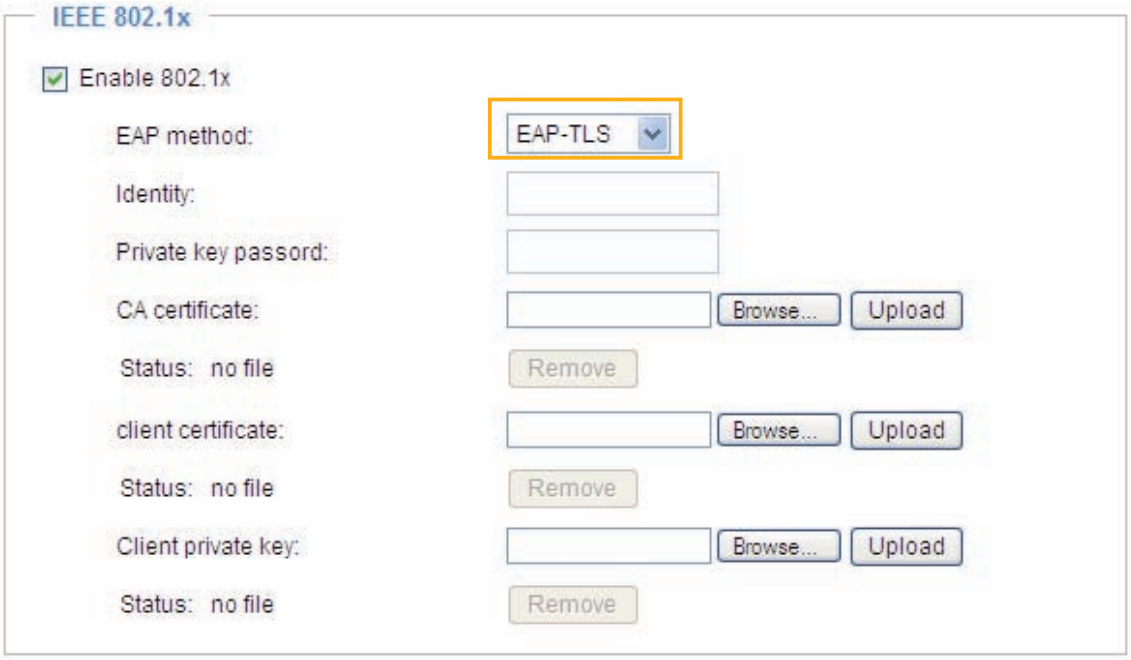
Authentication Server
(RADIUS Server)

1. Supplicant: A client end user (camera), which requests authentication.
2. Authenticator (an access point or a switch): A “go between” which restricts unauthorized end users from communicating with the authentication server.
3. Authentication server (usually a RADIUS server): Checks the client certificate and decides whether to accept the end user’s access request.

■ VIVOTEK Network Cameras support two types of EAP methods to perform authentication: **EAP-PEAP** and **EAP-TLS**.

Please follow the steps below to enable 802.1x settings:

1. Before connecting the Network Camera to the protected network with 802.1x, please apply a digital certificate from a Certificate Authority (ie. MIS of your company) which can be validated by a RADIUS server.
2. Connect the Network Camera to a PC or notebook outside of the protected LAN. Open the configuration page of the Network Camera as shown below. Select **EAP-PEAP** or **EAP-TLS** as the EAP method. In the following blanks, enter your ID and password issued by the CA, then upload related certificate(s).

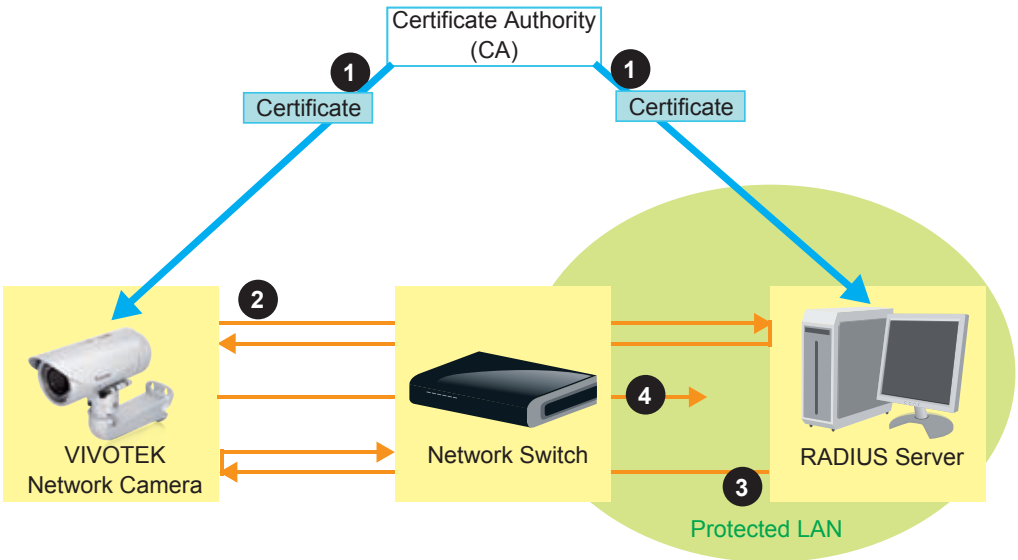


3. When all settings are complete, move the Network Camera to the protected LAN by connecting it to an 802.1x enabled switch. The devices will then start the authentication automatically.

NOTE

► The authentication process for 802.1x:

1. *The Certificate Authority (CA) provides the required signed certificates to the Network Camera (the supplicant) and the RADIUS Server (the authentication server).*
2. *A Network Camera requests access to the protected LAN using 802.1X via a switch (the authenticator). The client offers its identity and client certificate, which is then forwarded by the switch to the RADIUS Server, which uses an algorithm to authenticate the Network Camera and returns an acceptance or rejection back to the switch.*
3. *The switch also forwards the RADIUS Server's certificate to the Network Camera.*
4. *Assuming all certificates are validated, the switch then changes the Network Camera's state to authorized and is allowed access to the protected network via a pre-configured port.*



QoS (Quality of Service) Advanced Mode

Quality of Service refers to a resource reservation control mechanism, which guarantees a certain quality to different services on the network. Quality of service guarantees are important if the network capacity is insufficient, especially for real-time streaming multimedia applications. Quality can be defined as, for instance, a maintained level of bit rate, low latency, no packet dropping, etc.

The following are the main benefits of a QoS-aware network:
- The ability to prioritize traffic and guarantee a certain level of performance to the data flow.
- The ability to control the amount of bandwidth each application may use, and thus provide higher reliability and stability on the network.

Requirements for QoS

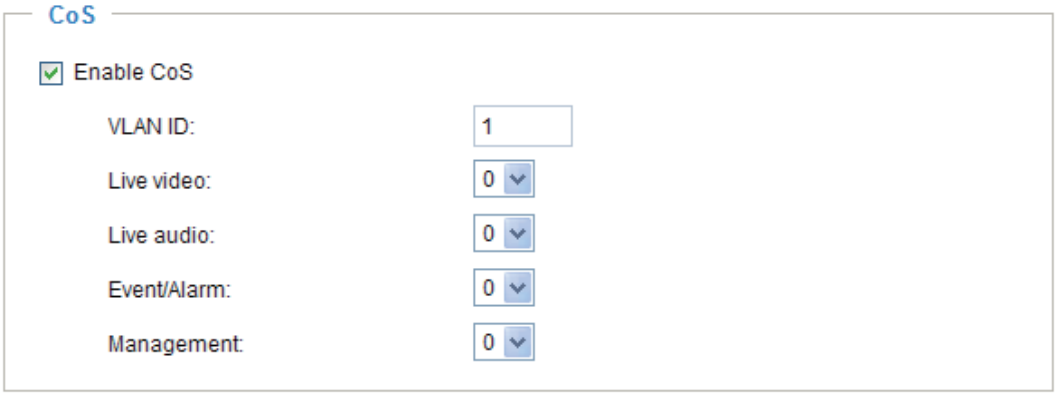
To utilize QoS in a network environment, the following requirements must be met:
- All network switches and routers in the network must include support for QoS.
- The network video devices used in the network must be QoS-enabled.

QoS models

CoS (the VLAN 802.1p model)

IEEE802.1p defines a QoS model at OSI Layer 2 (Data Link Layer), which is called CoS, Class of Service. It adds a 3-bit value to the VLAN MAC header, which indicates prioritization from 0~7 (Eight different classes of service are available). The priority is set up on the network switches, which then use different queuing disciplines to forward the packets.

Below is the setting column for CoS. Enter the **VLAN ID** of your switch (0~4095) and choose the priority for each application (0~7).



If you assign Video the highest level, the switch will handle video packets first.

NOTE

► *The web browsing may fail if the CoS setting is incorrect.*

► *Class of Service technologies do not guarantee a level of service in terms of bandwidth and delivery time; they offer a "best-effort." Users can think of CoS as "coarsely-grained" traffic control and QoS as "finely-grained" traffic control.*

► *Though CoS is simple to manage, it lacks scalability and does not offer end-to-end guarantees since it is based on L2 protocol.*

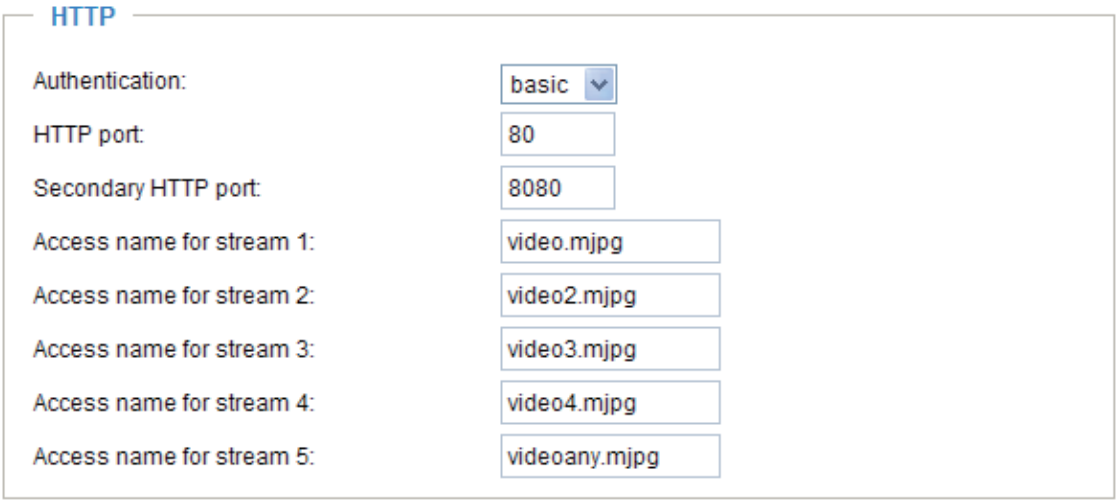
QoS/DSCP (the DiffServ model)

DSCP-ECN defines QoS at Layer 3 (Network Layer). The Differentiated Services (DiffServ) model is based on packet marking and router queuing disciplines. The marking is done by adding a field to the IP header, called the DSCP (Differentiated Services Codepoint). This is a 6-bit field that provides 64 different class IDs. It gives an indication of how a given packet is to be forwarded, known as the Per Hop Behavior (PHB). The PHB describes a particular service level in terms of bandwidth, queueing theory, and dropping (discarding the packet) decisions. Routers at each network node classify packets according to their DSCP value and give them a particular forwarding treatment; for example, how much bandwidth to reserve for it.

Below are the setting options of DSCP (DiffServ Codepoint). Specify the DSCP value for each application (0~63).

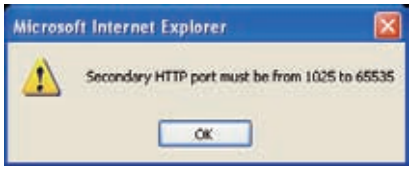
HTTP Advanced Mode

To utilize HTTP authentication, make sure that your have set a password for the Network Camera first; please refer to Security on page 31 for details.



Authentication: Depending on your network security requirements, the Network Camera provides two types of security settings for an HTTP transaction: basic and digest.
If **basic** authentication is selected, the password is sent in plain text format and there can be potential risks of being intercepted. If **digest** authentication is selected, user credentials are encrypted using MD5 algorithm and thus provide better protection against unauthorized accesses.

HTTP port / Secondary HTTP port: By default, the HTTP port is set to 80 and the secondary HTTP port is set to 8080. They can also be assigned to another port number between 1025 and 65535. If the ports are incorrectly assigned, the following warning messages will be displayed:



To access the Network Camera on the LAN, both the HTTP port and secondary HTTP port can be used to access the Network Camera. For example, when the HTTP port is set to 80 and the secondary HTTP port is set to 8080, refer to the list below for the Network Camera's IP address.

LAN
http://192.168.4.160 or http://192.168.4.160:8080

Access name for stream 1 ~ 5: This Network camera supports multiple streams simultaneously. The access name is used to differentiate the streaming source. Users can click **Configuration > Audio and Video > Video Settings** to set up the video quality of linked streams. For more information about how to set up the video quality, please refer to Viewing Windows on page 64.

When using Mozilla Firefox or Netscape to access the Network Camera and the video mode is set to JPEG, users will receive video comprised of continuous JPEG images. This technology, known as "server push", allows the Network Camera to feed live pictures to Mozilla Firefox and Netscape.

URL command -- http://<ip address>:<http port>/<access name for stream 1 ~ 5>
For example, when the Access name for stream 2 is set to video2.mjpg:
1. Launch Mozilla Firefox or Netscape.
2. Type the above URL command in the address bar. Press **Enter**.
3. The JPEG images will be displayed in your web browser.

NOTE

► *Microsoft® Internet Explorer does not support server push technology; therefore, using http://<ip address>:<http port>/<access name for stream 1 ~ 5> will fail to access the Network Camera.*

► *Users can only use URL commands to request the stream 5. For more information about URL commands, please refer to page 111.*

HTTPS

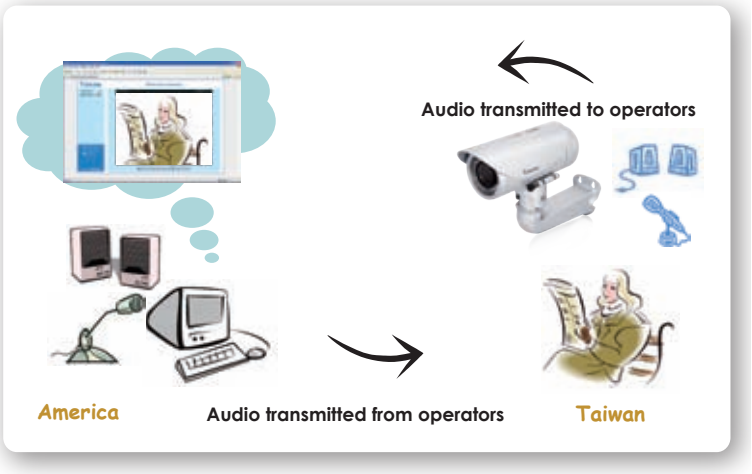
By default, the HTTPS port is set to 443. It can also be assigned to another port number between 1025 and 65535.

Two way audio

By default, the two way audio port is set to 5060. Also, it can also be assigned to another port number between 1025 and 65535.

The Network Camera supports two way audio communication so that operators can transmit and receive audio simultaneously. By using the Network Camera's built-in or external microphone and an external speaker, you can communicate with people around the Network Camera.

Note that as JPEG only transmits a series of JPEG images to the client, to enable the two-way audio function, make sure the video mode is set to “MPEG-4” on the Audio and Video Settings page and the media option is set to “Video and Audio” on the Client Settings page. Please refer to Client Settings on page 26 and Audio and Video Settings on page 58.



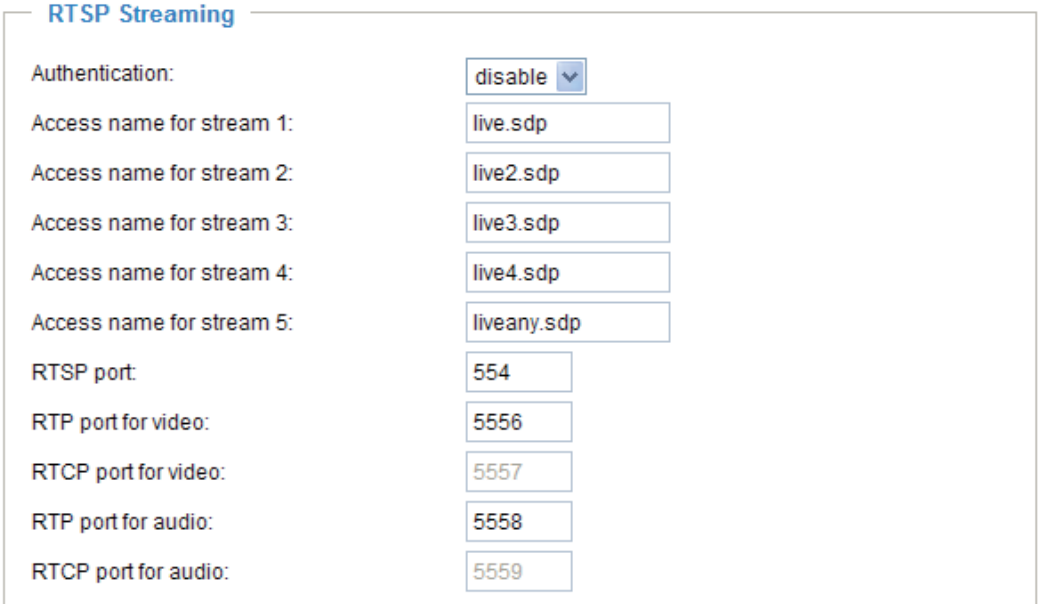
Click to enable audio transmission to the Network Camera; click to adjust the volume of microphone; click to turn off the audio. To stop talking, click again.

FTP

The FTP server allows the user to save recorded video clips. You can utilize VIVOTEK's Installation Wizard 2 to upgrade the firmware via FTP server. By default, the FTP port is set to 21. It also can be assigned to another port number between 1025 and 65535.

RTSP Streaming

To utilize RTSP streaming authentication, make sure that you have set a password for the Network Camera first; please refer to Security on page 31 for details.



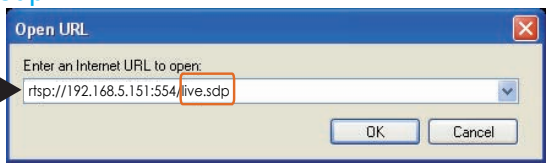
Authentication: Depending on your network security requirements, the Network Camera provides three types of security settings for streaming via RTSP protocol: disable, basic, and digest.
If **basic** authentication is selected, the password is sent in plain text format, but there can be potential risks of it being intercepted. If **digest** authentication is selected, user credentials are encrypted using MD5 algorithm, thus providing better protection against unauthorized access.
The availability of the RTSP streaming for the three authentication modes is listed in the following table:

	Quick Time player	Real Player
Disable	O	O
Basic	O	O
Digest	O	X

Access name for stream 1 ~ 5: This Network camera supports multiple streams simultaneously. The access name is used to differentiate the streaming source.

If you want to use an RTSP player to access the Network Camera, you have to set the video mode to MPEG-4 and use the following RTSP URL command to request transmission of the streaming data.
rtsp://<ip address>:<rtsp port>/<access name for stream1 ~ 5>
For example, when the access name for stream 1 is set to live.sdp:

1. Launch an RTSP player.
2. Choose File > Open URL. A URL dialog box will pop up.
3. Type the above URL command in the text box.
4. The live video will be displayed in your player as shown below.



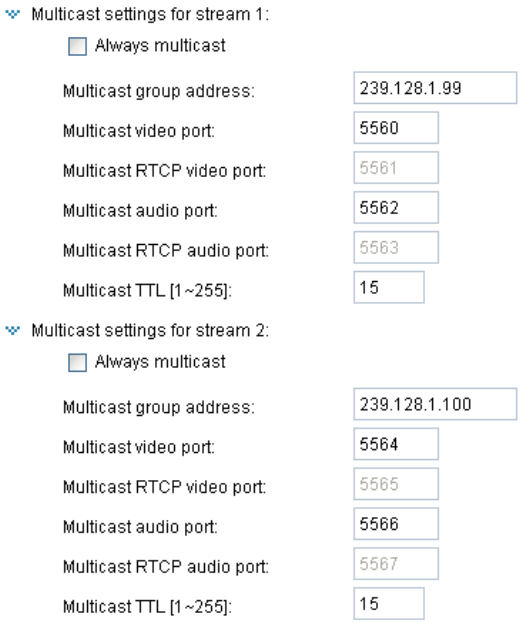
RTSP port /RTP port for video, audio/ RTCP port for video, audio

- RTSP (Real-Time Streaming Protocol) controls the delivery of streaming media. By default, the port number is set to 554.
- The RTP (Real-time Transport Protocol) is used to deliver video and audio data to the clients. By default, the RTP port for video is set to 5556 and the RTP port for audio is set to 5558.
- The RTCP (Real-time Transport Control Protocol) allows the Network Camera to transmit the data by monitoring the Internet traffic volume. By default, the RTCP port for video is set to 5557 and the RTCP port for audio is set to 5559.

The ports can be changed to values between 1025 and 65535. The RTP port must be an even number and the RTCP port is the RTP port number plus one, and thus is always an odd number. When the RTP port changes, the RTCP port will change accordingly.

If the RTP ports are incorrectly assigned, the following warning message will be displayed:

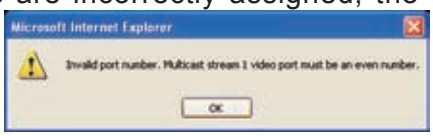
Multicast settings for stream 1 ~ 4: Click the items to display the detailed configuration information. Select the Always multicast option to enable multicast for stream 1 ~ 4.



Unicast video transmission delivers a stream through point-to-point transmission; multicast, on the other hand, sends a stream to the multicast group address and allows multiple clients to acquire the stream at the same time by requesting a copy from the multicast group address. Therefore, enabling multicast can effectively save Internet bandwith.

The ports can be changed to values between 1025 and 65535. The multicast RTP port must be an even number and the multicast RTCP port number is the multicast RTP port number plus one, and thus is always odd. When the multicast RTP port changes, the multicast RTCP port will change accordingly.

If the multicast RTP video ports are incorrectly assigned, the following warning message will be displayed:



Multicast TTL [1~255]: The multicast TTL (Time To Live) is the value that tells the router the range a packet can be forwarded.

DDNS

This section explains how to configure the dynamic domain name service for the Network Camera. DDNS is a service that allows your Network Camera, especially when assigned with a dynamic IP address, to have a fixed host and domain name.

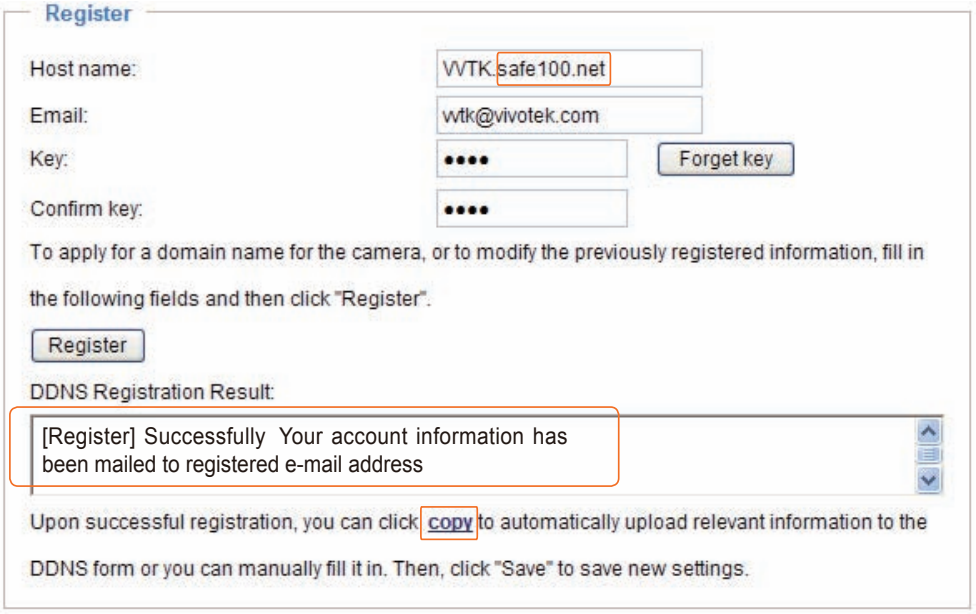
DDNS: Dynamic domain name service

Enable DDNS: Select this option to enable the DDNS setting.

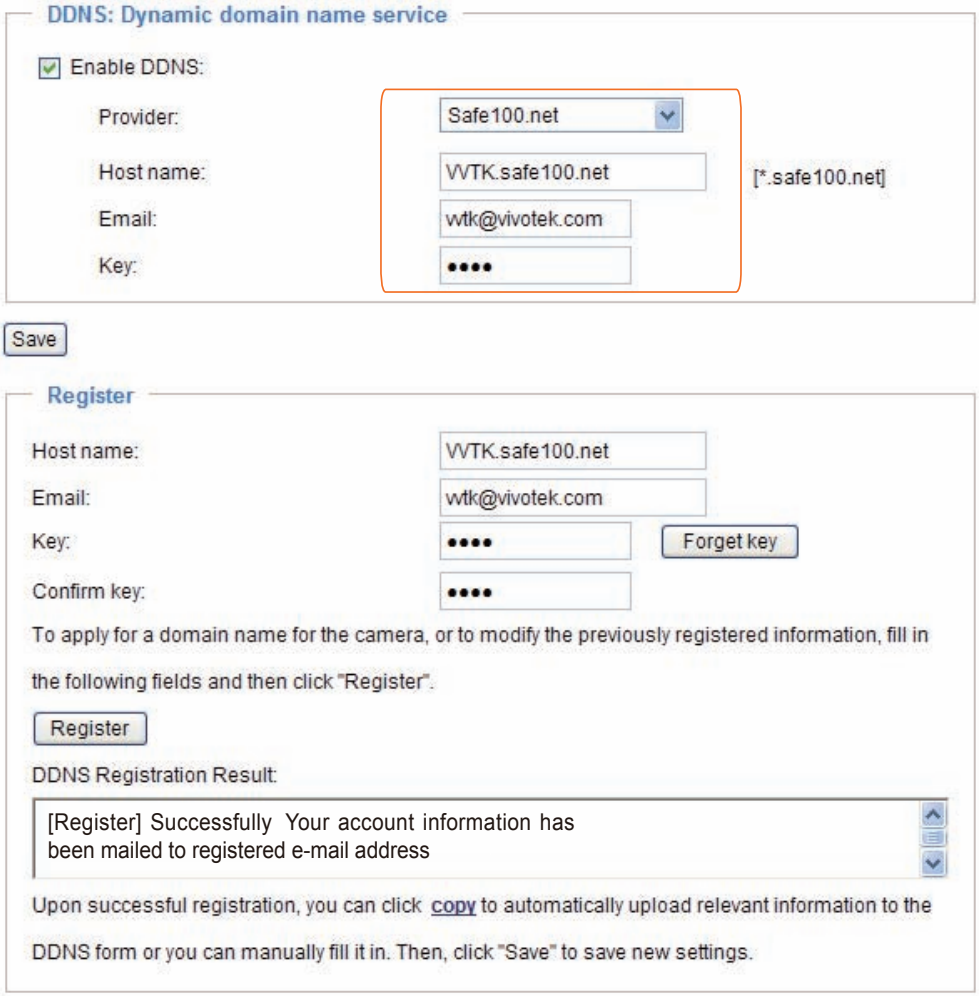
Provider: Select a DDNS provider from the provider drop-down list.
VIVOTEK offers **Safe100.net**, a free dynamic domain name service, to VIVOTEK customers. It is recommended that you register **Safe100.net** to access VIVOTEK's Network Cameras from the Internet. Additionally, we offer other DDNS providers, such as Dyndns.org(Dynamic), Dyndns.org(Custom), TZO.com, DHS.org, CustomSafe100, dyn-interfree.it.
Note that before utilizing this function, please apply for a dynamic domain account first.

■ Safe100.net

1. In the DDNS column, select **Safe100.net** from the drop-down list. Click **I accept** after reviewing the terms of the Service Agreement.
2. In the Register column, fill in the Host name (xxxx.safe100.net), Email, Key, and Confirm Key, and click **Register**. After a host name has been successfully created, a success message will be displayed in the DDNS Registration Result column.



3. Click **Copy** and all the registered information will automatically be uploaded to the corresponding fields in the DDNS column at the top of the page as seen in the picture.



4. Select Enable DDNS and click **Save** to enable the setting.

■ CustomSafe100

VIVOTEK offers documents to establish a CustomSafe100 DDNS server for distributors and system integrators. You can use CustomSafe100 to register a dynamic domain name if your distributor or system integrators offer such services.

1. In the DDNS column, select CustomSafe100 from the drop-down list.
2. In the Register column, fill in the Host name, Email, Key, and Confirm Key; then click **Register**. After a host name has been successfully created, you will see a success message in the DDNS Registration Result column.
3. Click **Copy** and all for the registered information will be uploaded to the corresponding fields in the DDNS column.
4. Select Enable DDNS and click **Save** to enable the setting.

Forget key: Click this button if you have forgotten the key to Safe100.net or CustomSafe100. Your account information will be sent to your email address.

Refer to the following links to apply for a dynamic domain account when selecting other DDNS providers:

■ Dyndns.org(Dynamic) / Dyndns.org(Custom): visit http://www.dyndns.com/
■ TZO.com: visit http://www.tzo.com/
■ DHS.org: visit http://www.dhs.org/
■ dyn-interfree.it: visit http://dyn-interfree.it/

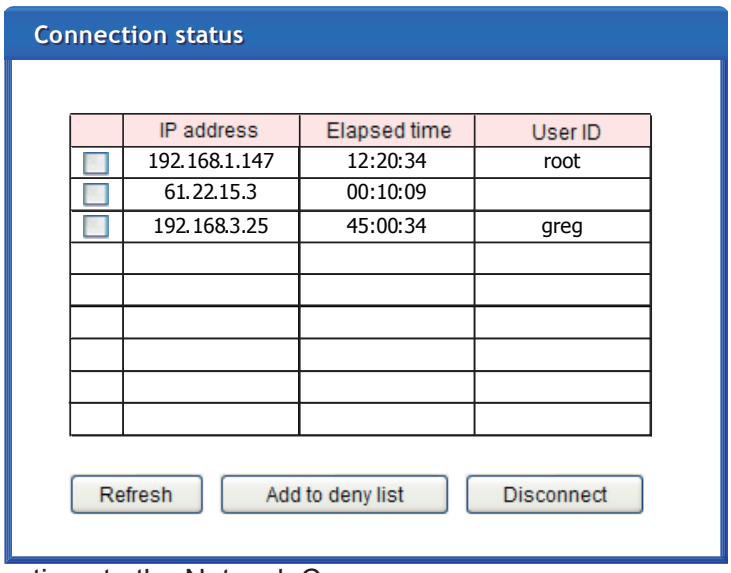
Access List Advanced Mode

This section explains how to control access permission by verifying the client PC's IP address.

General Settings

Maximum number of concurrent streaming connection(s) limited to: Simultaneous live viewing for 1~10 clients (including stream 1 and stream 2). The default value is 10. If you modify the value and click **Save**, all current connections will be disconnected and automatically attempt to re-link (IE Explore or Quick Time Player).

View Information: Click this button to display the connection status window showing a list of the current connections. For example:



■ IP address: Current connections to the Network Camera.

■ Elapsed time: How much time the client has been at the webpage.

■ User ID: If the administrator has set a password for the webpage, the clients have to enter a user name and password to access the live video. The user name will be displayed in the User ID column. If the administrator allows clients to link to the webpage without a user name and password, the User ID column will be empty.

There are some situations which allow clients access to the live video without a user name and password:

1. The administrator does not set up a root password. For more information about how to set up a root password and manage user accounts, please refer to Security on page 31.
2. The administrator has set up a root password, but set **RTSP Authentication** to "disable". For more information about **RTSP Authentication**, please refer to RTSP Streaming on page 51.
3. The administrator has set up a root password, but allows anonymous viewing. For more information about **Allow Anonymous Viewing,** please refer to Security on page 31.

■ Refresh: Click this button to refresh all current connections.

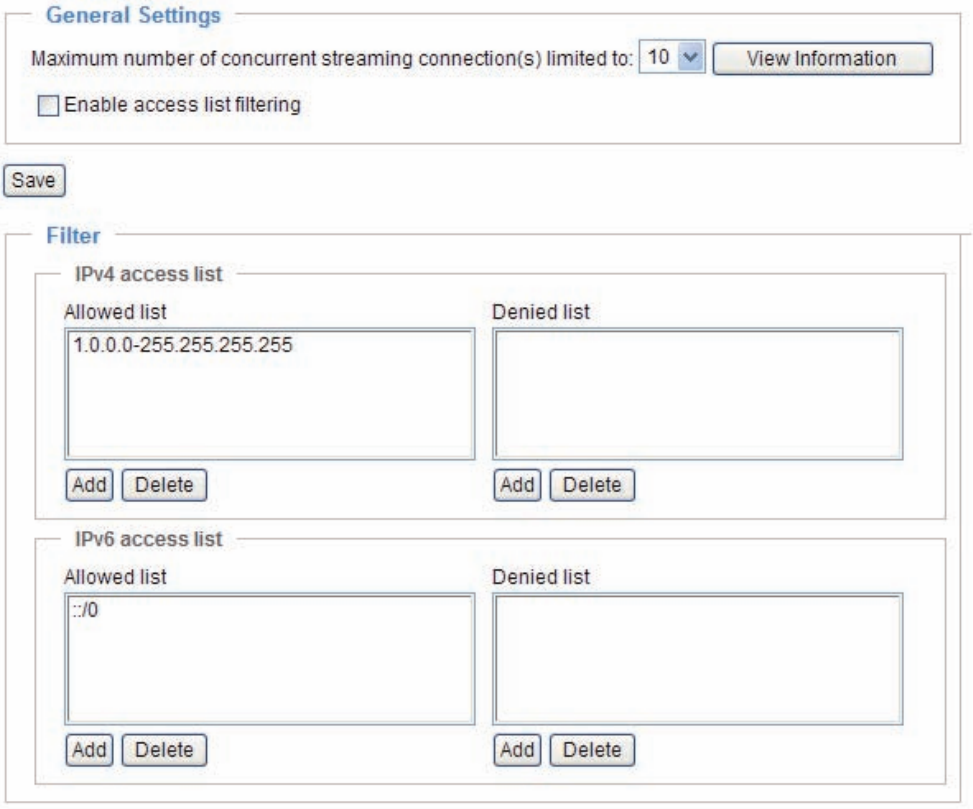
■ Add to deny list: You can select entries from the Connection Status list and add them to the Deny List to deny access. Please note that those checked connections will only be disconnected temporarily and will automatically try to re-link again (IE Explore or Quick Time Player). If you want to enable the denied list, please check **Enable access list filtering** and click **Save** in the first column.

■ Disconnect: If you want to break off the current connections, please select them and click this button. Please note that those checked connections will only be disconnected temporarily and will automatically try to re-link again (IE Explore or Quick Time Player).

Enable access list filtering: Check this item and click **Save** if you want to enable the access list filtering function.

Filter

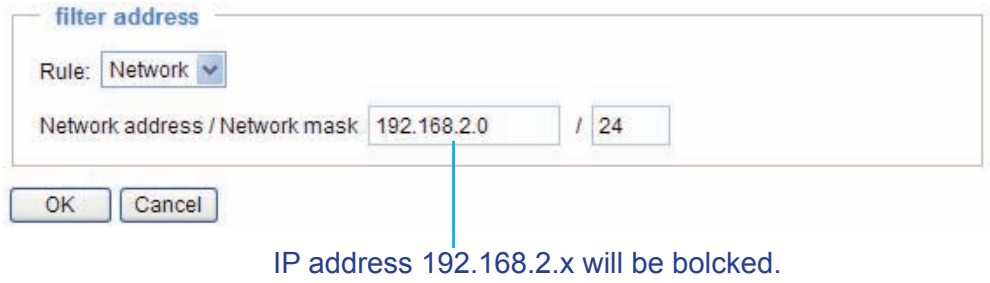
There are two lists for permission control: Allowed list and Denied list. Only those clients whose IP addresses are on the Allowed list and not on the Denied list can access the Network Camera. Please note that the IPv6 access list column will not be displayed unless you enable IPv6 on the Network page. For more information about **IPv6 Settings**, please refer to page 42 for detailed information.



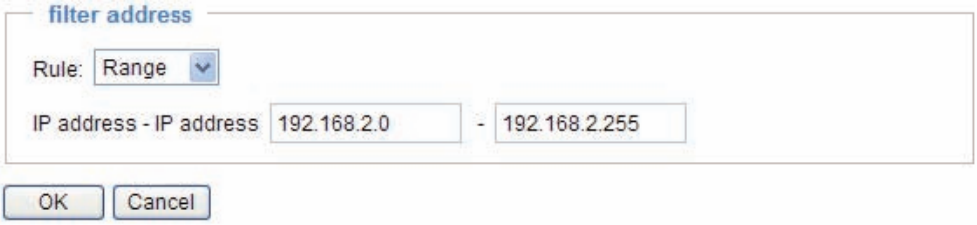
■ Add a rule to Allowed/Denied list: Click **Add** to add a rule to Allowed/Denied list.

There are three types of rules:
Single: This rule allows the user to add an IP address to the Allowed/Denied list.
For example:

Network: This rule allows the user to assign a network address and corresponding subnet mask to the Allow/Deny List.
For example:



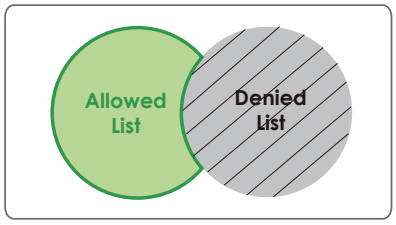
Range: This rule allows the user to assign a range of IP addresses to the Allow/Deny List. This rule is only applied to IPv4.
For example:



■ Delete Allowed/Denied list:
In the Delete Allowed List or Delete Denied List column, make a selection and click **Delete**.

NOTE

► *For example, when the range of IP addresses on the allowed list is set from 1.1.1.0 to 192.255.255.255 and the range in the denied list is set from 1.1.1.0 to 170.255.255.255, only users' IPs between 171.0.0.0 and 192.255.255.255 can access the Network Camera.*



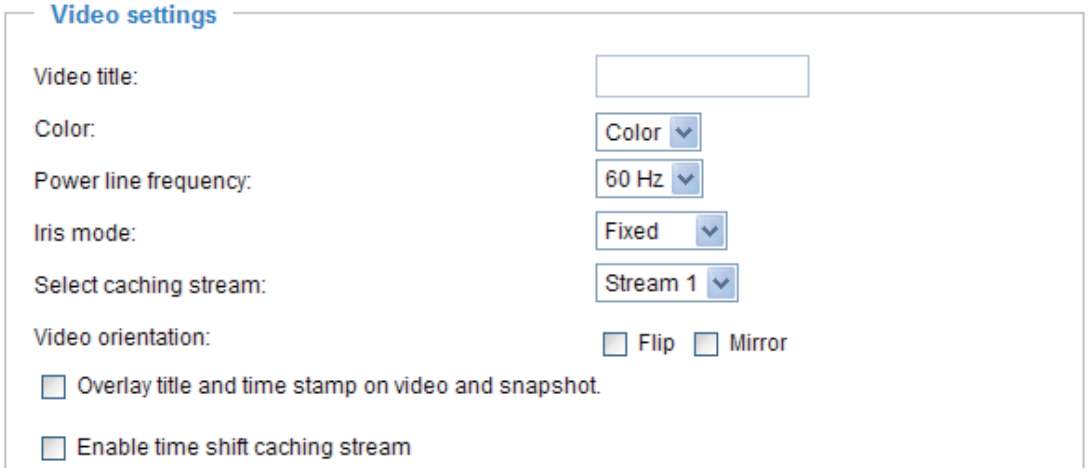
Administrator IP address

Always allow the IP address to access this device: You can check this item and add the Administrator's IP address in this field to make sure the Administrator can always connect to the device.

Audio and Video

This section explains how to cofigure the audio and video settings of the Network Camera. It is composed of the following two columns: Video Settings and Audio Settings.

Video Settings



Video title: Enter a name that will be displayed on the title bar of the live video.

Color: Select to display color or black/white video streams.

Power line frequency: Set the power line frequency consistent with local utility settings to eliminate image flickering associated with fluorescent lights. Note that after the power line frequency is changed, you must disconnect and reconnect the power cord of the Network Camera in order for the new setting to take effect.

Iris mode: Select a proper iris mode for your environment.

Select caching stream: This Network Camera supports time shift cache stream on the Network Camera. Select one stream and check the below option **Enable time shift caching stream**.

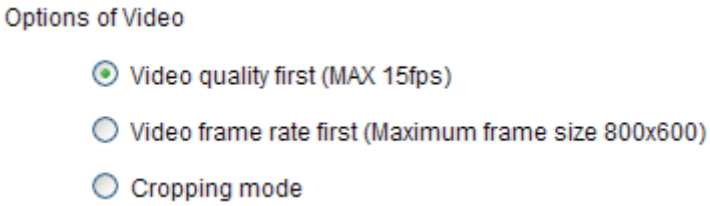
Enable time shift caching stream Advanced Mode: Check this item to enable the time shift cache stream on the Network Camera, which will stores video in the camera's embedded memory for a period of time depending on the cache memory of each Network Camera. This function can work seamlessly with VIVOTEK's ST7501 recording software. When an event occurs, the recording software can request time shift cache stream from the camera, which allows the user to get an earlier video data.

Video orientation: Flip--vertically reflect the display of the live video; Mirror--horizontally reflect the display of the live video. Select both options if the Network Camera is installed upside-down (ex. on the ceiling) to correct the image orientation. Please note that the preset locations will be cleared after flip/mirror.

Overlay title and time stamp on video: Select this option to place the video title and time on the video streams.
Note that when the frame size is set to 176 x 144 as shown in the picture below, only the time will be stamped on the video streams.

Options of Video Advanced Mode

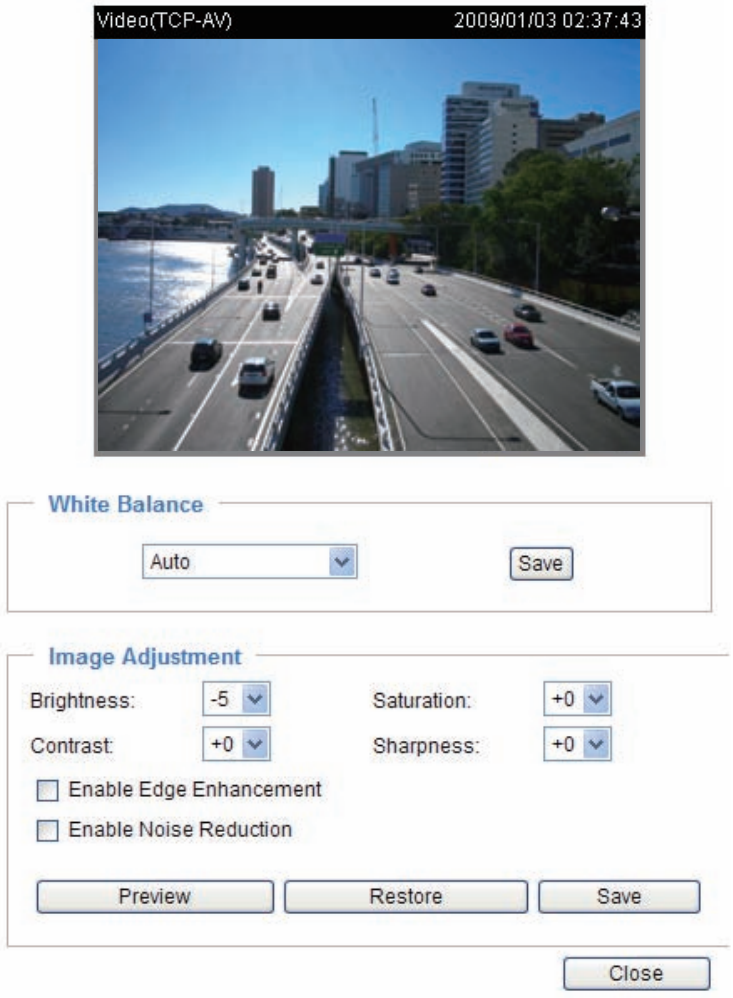
There are three options for you to choose: **Video quality first**, **Video frame rate first**, and **Cropping mode**. Select either one mode according to your needs.



- Video quality first: Select this option will reduce the maximum frame rate to 15fps and clear the settings in the Viewing Window.
- Video frame rate first: Select this option will limit the frame size to 800x600 and clear the settings in the Viewing Window.
- Cropping mode: The cropping function allows users to crop unnecessary information and simply transmit the image of the target region for live viewing or storage. With the trimming, the transmitting data size and thus, the network load is reduced and a higher frame rate is obtained. As a result, bandwidth resources and storage space can be used more efficiently.

Image Settings Advanced Mode

Click **Image Settings** to open the Image Settings page. On this page, you can tune the White balance, Brightness, Saturation, Contrast, and Sharpness settings for the video.



White balance: Adjust the value for the best color temperature.

■ Auto
The Network Camera automatically adjusts the color temperature of the light in response to different light sources. The white balance setting defaults to **Auto** and works well in most situations.

■ Keep current value
Follow the steps below to manually set the white balance to compensate for the ambient lighting conditions.
1. Set the White balance to **Auto** and click **Save**.
2. Place a sheet of white paper in front of the lens, then allow the Network Camera to adjust the color temperature automatically.
3. Select Keep Current Value to confirm the setting while the white balance is being measured.
4. Click **Save** to enable the new setting.

Image Adjustment

■ Brightness: Adjust the image brightness level, which ranges from -5 to +5.

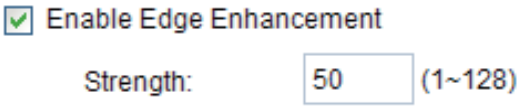
■ Saturation: Adjust the image saturation level, which ranges from -5 to +5.

■ Contrast: Adjust the image contrast level, which ranges from -5 to +5.

■ Sharpness: Adjust the image sharpness level, which ranges from -5 to +5.

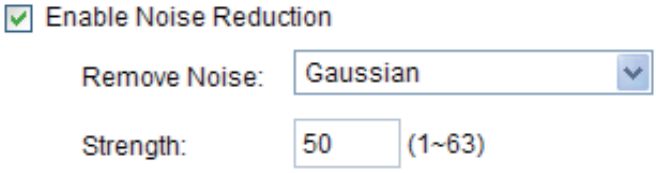
Enable Edge Enhancement

Edge enhancement is an image processing filter that enhances the edge contrast of an image or video to improve its sharpness. Enter a value from 1 to 128 to set the degree of enhancement desired.



Enable Noise Reduction

Noise reduction is the process of removing noise from a signal. Select the type of noise to remove and enter a value from 1 to 63 to set the degree of enhancement required.



You can click **Preview** to fine-tune the image, or click **Restore** to recall the original settings without incorporating the changes. When completed with the settings on this page, click **Save** to enable the setting and click **Close** to exit the page.

Privacy Mask Advanced Mode

Click **Privacy Mask** to open the settings page. On this page, you can block out sensitive zones to address privacy concerns.

■ To set the privacy mask windows, follow the steps below:

1. Click **New** to add a new window.
2. Use the mouse to size and drag-drop the window, which is recommended to be at least twice the size of the object (height and width) you want to cover.
3. Enter a Window Name and click **Save** to enable the setting.
4. Select **Enable privacy mask** to enable this function.

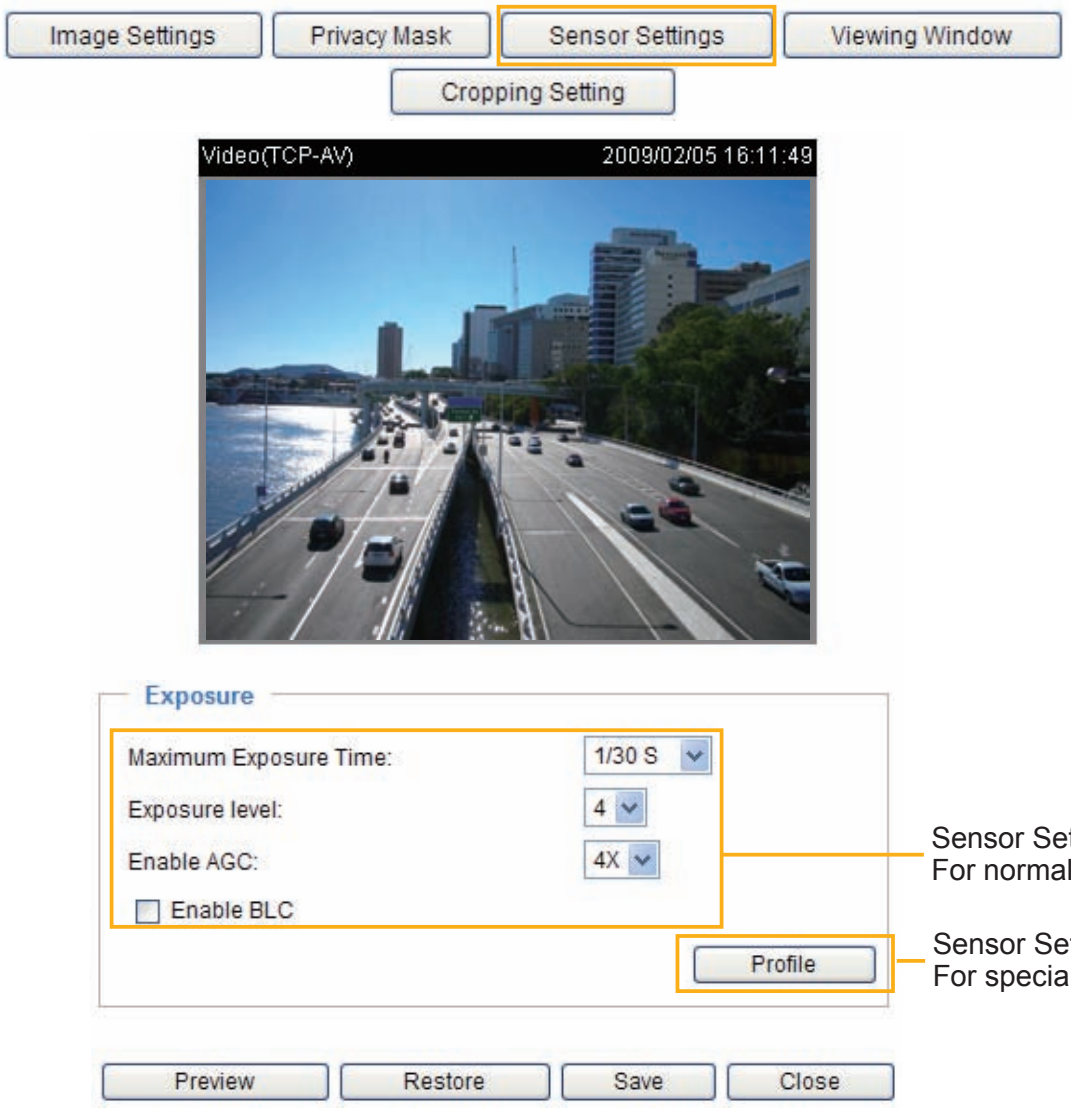
NOTE

► *Up to 5 privacy mask windows can be set up on the same screen.*

► *If you want to delete the privacy mask window, please click the 'x' on the upper right-hand corner of the window.*

Sensor Settings Advanced Mode

Click **Sensor Settings** to open the Sensor Settings page. On this page, you can set the maximum exposure time, exposure level, and AGC (Auto Gain Control) settings.
You can configure two sets of sensor settings: one for normal situations, the other for special situations, such as day/night/schedule mode.



Exposure

- Maximum Exposure Time: Select a proper maximum exposure time according to the light source of the surroundings. The exposure times are selectable for the following durations: 1/120 second, 1/60 second, 1/30 second, 1/15 second, and 1/5 second. Shorter exposure time results in less light.

- Exposure level: You can manually set the Exposure level, which ranges from 1 to 8 (dark to bright).The default value is 4.

- Enable AGC (Auto Gain Control): You can manually set the AGC level (2X 4X, or 8X). The default value is 4X.

- Enable BLC (Back Light Compensation): Enable this option when the object is too dark or too bright to recognize. It allows the camera to adjust to the best light conditions in any environment and automatically give the necessary light compensation.

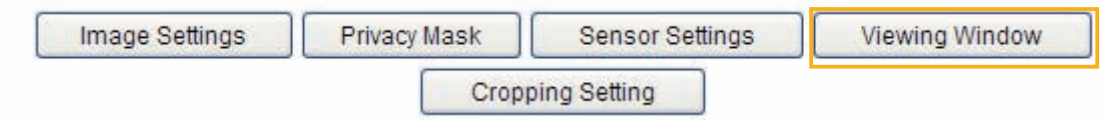
You can click **Preview** to fine-tune the image, or click **Restore** to recall the original settings without incorporating the changes. When completed with the settings on this page, click **Save** to enable the settings and click **Close** to exit the page.

If you want to configure another sensor setting for day/night/schedule mode, please click **Profile** to open the Sensor Settings Profile Settings page as shown below.

Please follow the steps beolw to setup a profile:

1. Check **Enable this profile**.
2. Select the applied mode: Day mode, Night mode, or Schedule mode. Please manually enter a range of time if you choose Schedule mode.
3. Configure Exposure settings in the second column. Please refer to last page for detailed information.
4. Click **Save** to enable the setting and click **Close** to exit the page.

Viewing Window Advanced Mode
Click **Viewing Window** to open the Viewing Window Settings page.



This Network Camera supports multiple streams with frame size ranging from 176 x 144 to 1600 x 1200.

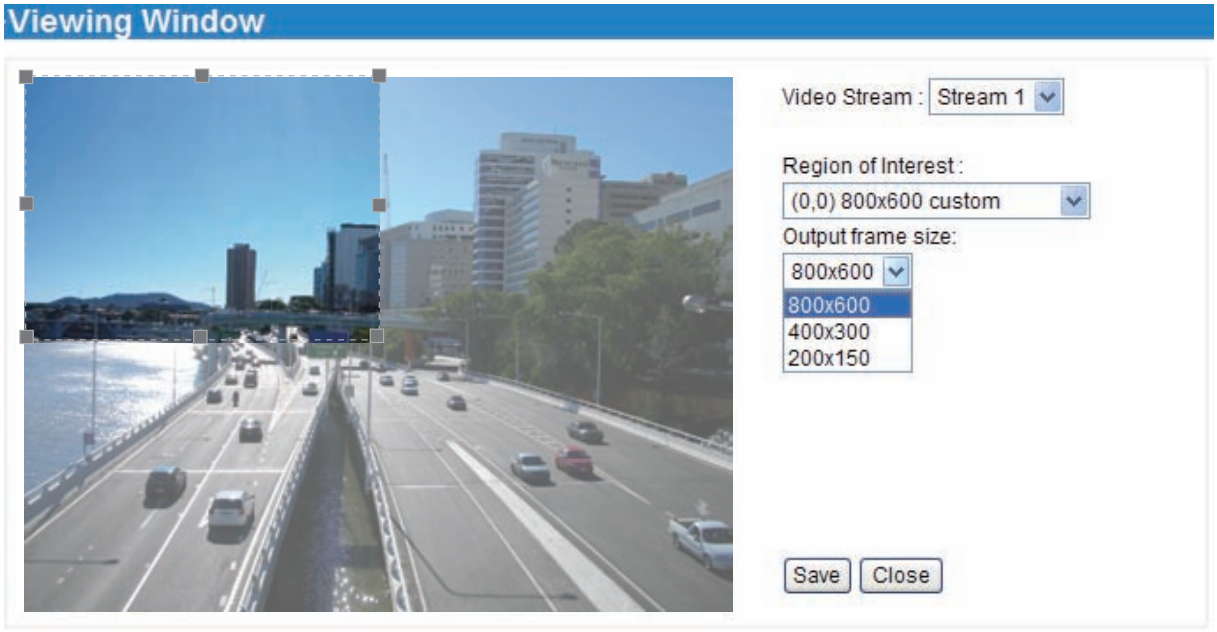
The definition of multiple streams:

- Stream 1: Users can define the "Region of Interest" (viewing region) and the "Output Frame Rate" (size of the live view window).
- Stream 2: Users can define the "Region of Interest" (viewing region) and the "Output Frame Rate" (size of the live view window).
- Stream 3 (Mobile stream): Users can define the "Region of Interest" (viewing region), but the "Output Frame Rate" (size of the live view window) is fixed at 176 x 144.
- Stream 4 (Global view stream): This stream captures the full view of the video and streams out at the maximum resolution (1600 x 1200).

NOTE

► *All the items in the "Region of Interest" should not be greater than the "Output Frame Size" (current maximum resolution).*

Click **Viewing Window** to open the viewing region settings page. On this page, you can set the **Region of Interest** and the **Output Frame Size** for stream 1 ~ 3.



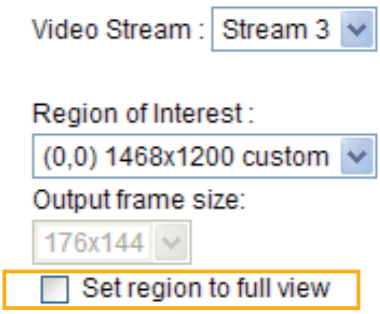
Please follow the steps below to set up those settings for a stream:

1. Select a stream which you want to set up the viewing region. If you want to stream out the video to a mobile device, please select stream 3.
2. Select a **Region of Interest** from the drop-down list. The floating frame, the same as the one in the Global View window on the home page, will resize accordingly. If you want to set up a customized viewing region, you can also resize and drag the floating frame to a desired position with your mouse.
3. Choose a proper **Output Frame Size** from the drop-down list according to the size of your monitoring device.

■ The parameters of the multiple streams:

	Region of Interest	Output frame size
Stream 1	1600 X 1200 ~ 176 x 144 (Selectable)	1600 X 1200 ~ 176 x 144 (Selectable)
Stream 2	1600 X 1200 ~ 176 x 144 (Selectable)	1600 X 1200 ~ 176 x 144 (Selectable)
Stream 3	1468 x 1200 ~ 176 x 144 (Selectable)	176 x 144 (Fixed)
Stream 4	1600 X 1200 (Fixed)	1600 X 1200 (Fixed)

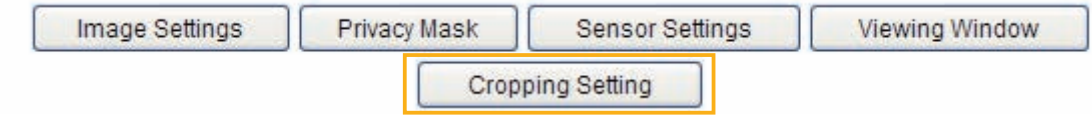
■ The maximum **Region of Interest** of stream 3 is 1468 x 1200. You can also check the item "Set region to full view" to extend the region to full view (1600 x 1200). However, the image will be distorted a little bit.



When completed with the settings in the Viewing Window, click **Save** to enable the settings and click **Close** to exit the window. The selected **Output Frame Size** will immediately be applied to the **Frame size** of each video stream as shown on page 62. Then you can go back to the home page to test the e-PTZ function. For more information about the e-PTZ function, please refer to page 80.

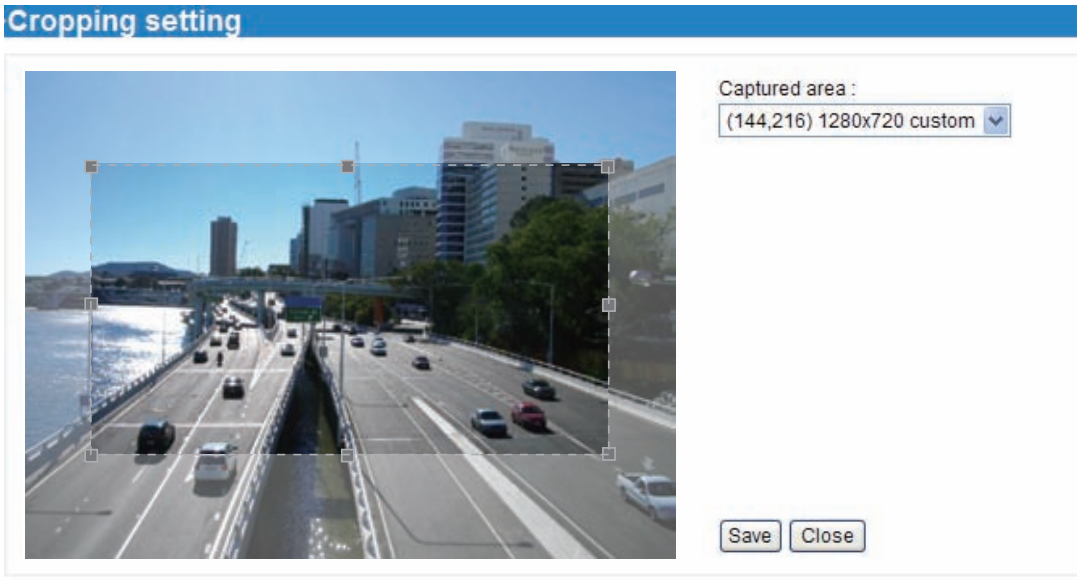
Cropping Setting Advanced Mode

Click **Cropping Setting** to open the Cropping Settings page.

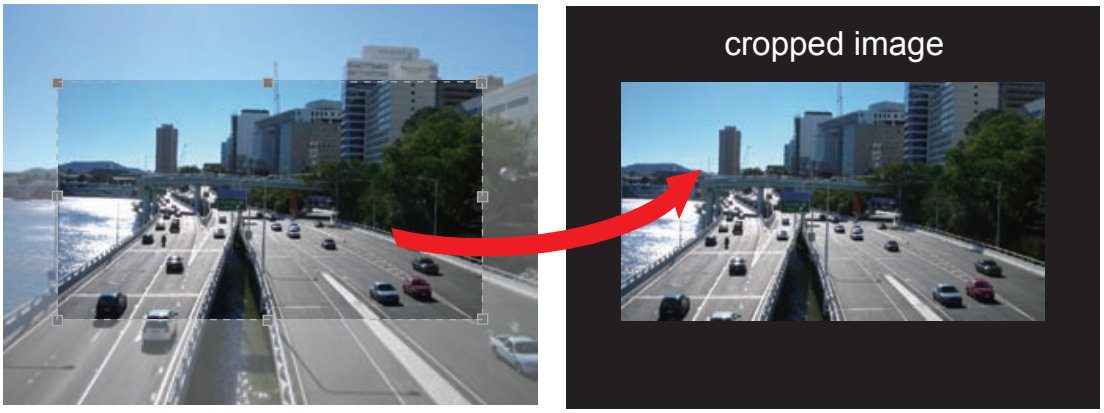


Please follow the steps below to set up cropping mode for mutiple streams:

1. Click **Cropping Setting** to open the window as shown below.
2. Select a **Captured area** from the drop-down list. The floating frame, the same as the one in the Global View window on the home page, will resize accordingly. If you want to set up a customized viewing region, you can also resize and drag the floating frame to a desired position with your mouse.



3. Click **Save** to enable the settings and click **Close** to exit the window. Below is the illustration of cropped image:



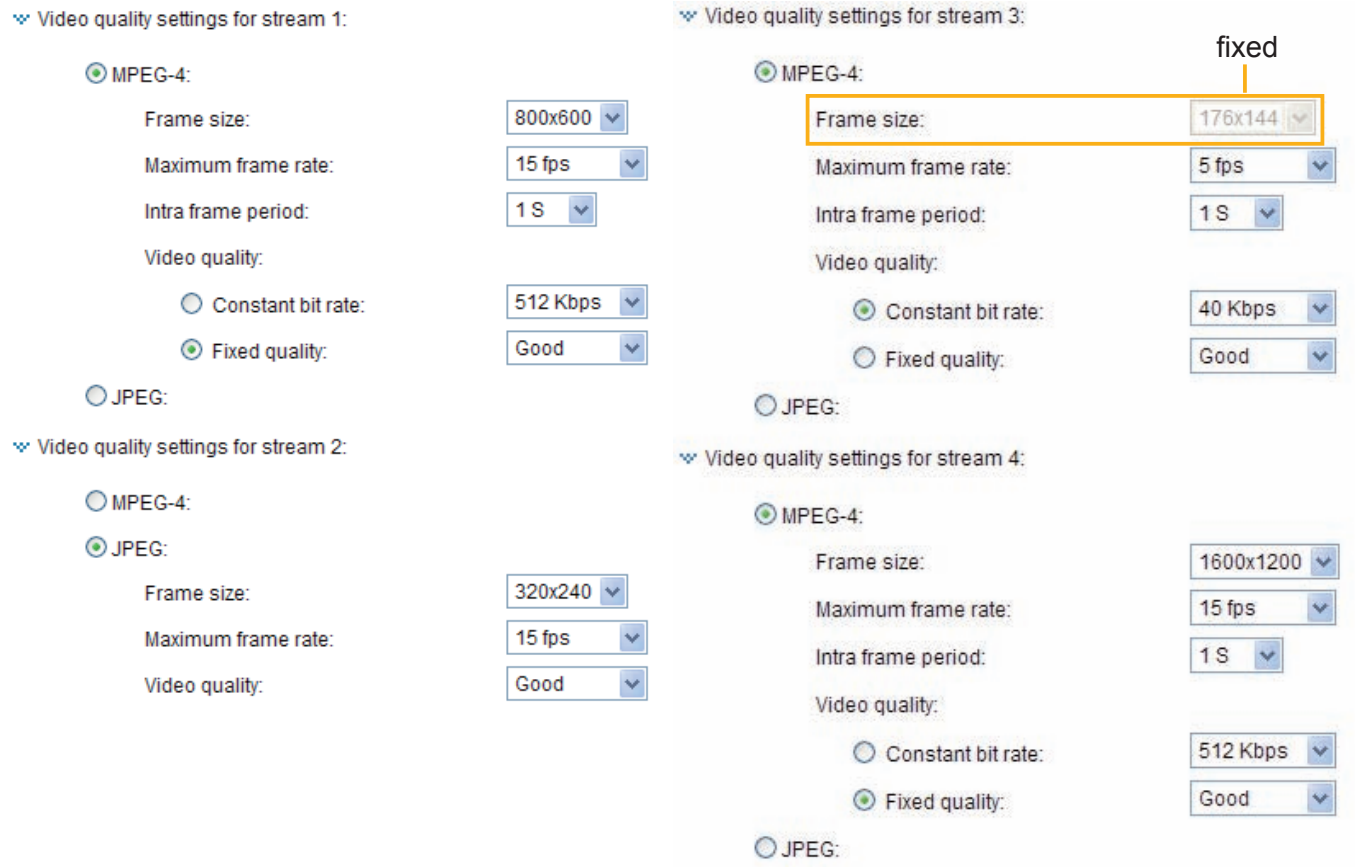
NOTE

► *In cropping mdoe, the maximum frame rate will be up to 30fps if the width is under 1280 and the height is under 720; otherwise, the maximum frame rate may be reduced to 15fps.*

► *Select cropping mode will clear the settings in the Viewing Window and disable Motion Detection, Privacy Mask, and Preset Position.*

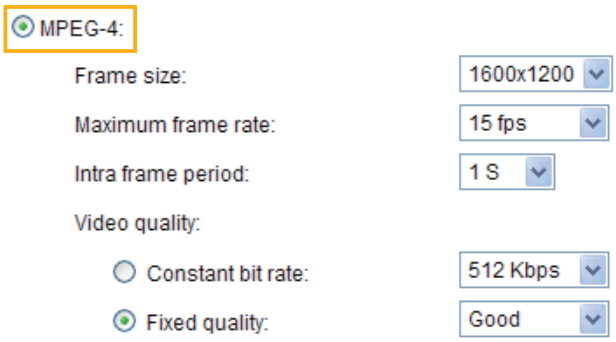
Video Quality Settings

Click the stream item to display the detailed information. The maximum frame size will follow your settings in above sections.



This Network Camera offers real-time MPEG-4 and MJEPG compression standards (dual codec) for real-time viewing.

If **MPEG-4** mode is selected, the video is streamed via RTSP protocol. There are four parameters for you to adjust the video performance:



■ Frame size

You can set up different video resolution for different viewing devices. For example, set a smaller frame size and lower bit rate for remote viewing on mobile phones and a larger video size and a higher bit rate for live viewing on web browsers. Note that a larger frame size takes up more bandwidth.

■ Maximum frame rate

This limits the maximum refresh frame rate per second. Set the frame rate higher for smoother video quality.

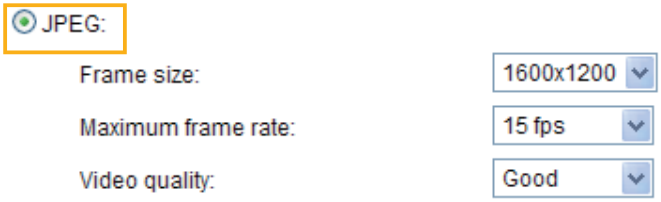
If the power line frequency is set to 50Hz, the frame rates are selectable at 1fps, 2fps, 3fps, 5fps, 8fps, 10fps, 15fps, 20fps, and 25fps. If the power line frequency is set to 60Hz, the frame rates are selectable at 1fps, 2fps, 3fps, 5fps, 8fps, 10fps, 15fps, 20fps, 25fps, and 30fps. You can also select **Customize** and manually enter a value. The frame rate will decrease if you select a higher resolution.

■ Intra frame period
Determine how often to plant an I frame. The shorter the duration, the more likely you will get better video quality, but at the cost of higher network bandwidth consumption. Select the intra frame period from the following durations: 1/4 second, 1/2 second, 1 second, 2 seconds, 3 seconds, and 4 seconds.

■ Video quality
A complex scene generally produces a larger file size, meaning that higher bandwidth will be needed for data transmission. Therefore, if **Constant bit rate** is selected, the bandwidth utilization is fixed at a selected level, resulting in mutable video quality performance. The bit rates are selectable at the following rates: 20Kbps, 30Kbps, 40Kbps, 50Kbps, 64Kbps, 128Kbps, 256Kbps, 512Kbps, 768Kbps, 1Mbps, 2Mbps, 3Mbps, and 4Mbps. You can also select **Customize** and manually enter a value.

On the other hand, if **Fixed quality** is selected, all frames are transmitted with the same quality; bandwidth utilization is therefore unpredictable. The video quality can be adjusted to the following settings: Medium, Standard, Good, Detailed, and Excellent. You can also select **Customize** and manually enter a value.

If **JPEG** mode is selected, the Network Camera continuously sends JPEG images to the client, producing a moving effect similar to a filmstrip. Every single JPEG image transmitted guarantees the same image quality, which in turn comes at the expense of variable bandwidth usage. Because the media contents are a combination of JPEG images, no audio data is transmitted to the client. There are three parameters provided in MJPEG mode to control the video performance:



■ Frame size
You can set up different video resolution for different viewing devices. For example, set a smaller frame size and lower bit rate for remote viewing on mobile phones and a larger video size and a higher bit rate for live viewing on web browsers. Note that a larger frame size takes up more bandwidth.

■ Maximum frame rate
This limits the maximum refresh frame rate per second. Set the frame rate higher for smoother video quality.
If the power line frequency is set to 50Hz, the frame rates are selectable at 1fps, 2fps, 3fps, 5fps, 8fps, 10fps, 15fps, 20fps, and 25fps. If the power line frequency is set to 60Hz, the frame rates are selectable at 1fps, 2fps, 3fps, 5fps, 8fps, 10fps, 15fps, 20fps, 25fps, and 30fps. You can also select **Customize** and manually enter a value. The frame rate will decrease if you select a higher resolution.

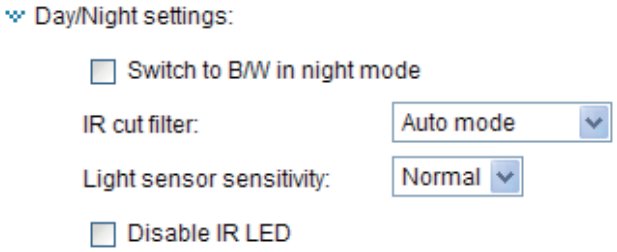
■ Video quality
The video quality can be adjusted to the following settings: Medium, Standard, Good, Detailed, and Excellent. You can also select **Customize** and manually enter a value.

NOTE

► *Video quality and fixed quality refers to the **compression rate**, so a lower value will produce higher quality.*

► *Converting high-quality video may significantly increase the CPU loading, and you may encounter streaming disconnection or video loss while capturing a complicated scene. In the event of occurance, we suggest you customize a lower video resolution or reduce the frame rate to obtain smooth video.*

Day/Night Settings



Switch to B/W in night mode
Select this to enable the Network Camera to automatically switch to B/W during night mode.

IR cut filter
With a removable IR-cut filter, this Network Camera can automatically remove the filter to let IR light into the sensor during low light conditions.

■ Auto mode
The Network Camera automatically removes the filter by judging the level of ambient light.

■ Day mode
In day mode, the Network Camera switches on the IR cut filter at all times to block infrared light from reaching the sensor so that the colors will not be distorted.

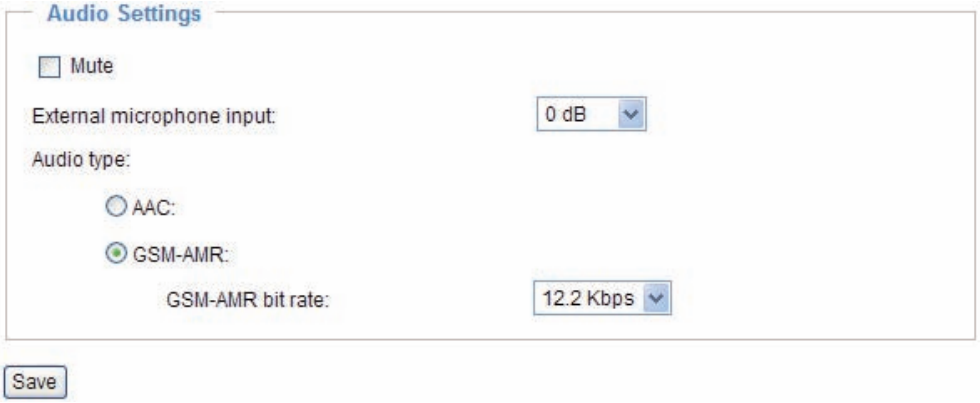
■ Night mode
In night mode, the Network Camera switches off the IR cut filter at all times for the sensor to accept infrared light, thus helping to improve low light sensitivity.

■ Schedule mode
The Network Camera switches between day mode and night mode based on a specified schedule. Enter the start and end time for day mode. Note that the time format is [hh:mm] and is expressed in 24-hour clock time. By default, the start and end time of day mode are set to 07:00 and 18:00.

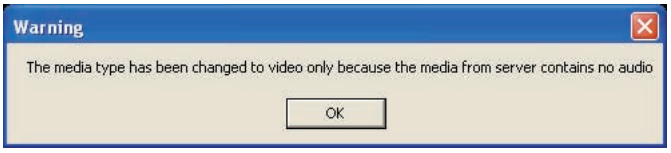
Light sensor sensitivity
Select Low, Normal, or High sensitivity for the light sensor.

Disable IR LED
If you do not want to use the IR illuminators, you can select this option to turn it off.

Audio Settings



Mute: Select this option to disable audio transmission from the Network Camera to all clients. Note that if mute mode is turned on, no audio data will be transmitted even if audio transmission is enabled on the Client Settings page. In that case, the following message is displayed:



External microphone input: Select the gain of the external audio input according to ambient conditions. Adjust the gain from +21 db (most sensitive) or -33 db (least sensitive).

Audio type: Select audio codec AAC or GSM-AMR and the bit rate.

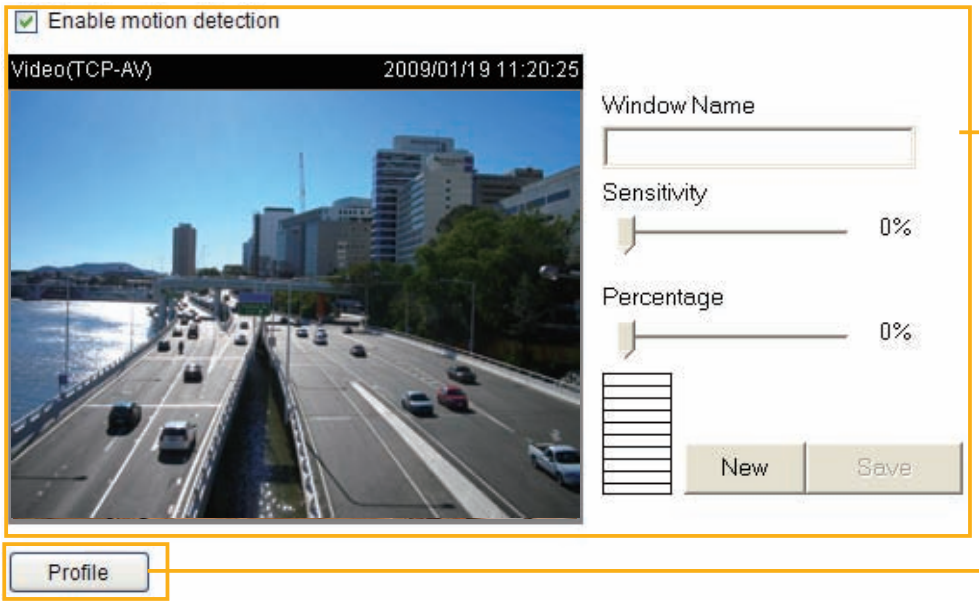
- AAC provides good sound quality at the cost of higher bandwidth consumption. The bit rates are selectable from: 16Kbps, 32Kbps, 48Kbps, 64Kbps, 96Kbps, and 128Kbps.

- GSM-ARM is designed to optimize speech quality and requires less bandwidth. The bit rates are selectable from: 4.75Kbps, 5.15Kbps, 5.90Kbps, 6.7Kbps, 7.4Kbps, 7.95Kbps, 10.2Kbps, and 12.2Kbps.

When completed with the settings on this page, click **Save** to enable the settings.

Motion Detection

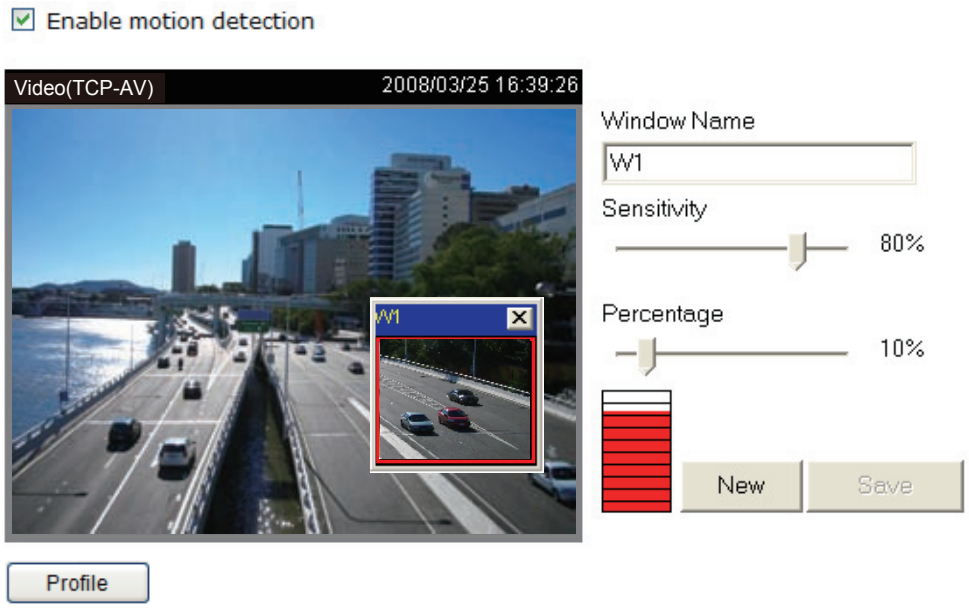
This section explains how to configure the Network Camera to enable motion detection. A total of three motion detection windows can be configured.



Follow the steps below to enable motion detection:

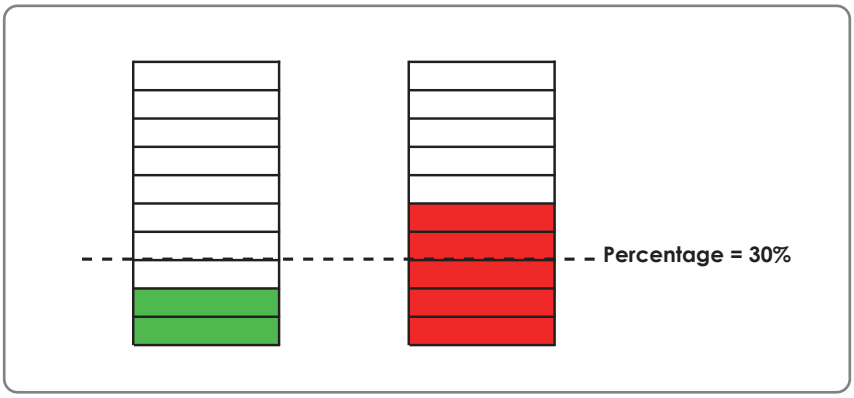
1. Click **New** to add a new motion detection window.
2. In the Window Name text box, enter a name for the motion detection window.
   - To move and resize the window, drag and drop your mouse on the window.
   - To delete window, click X on the top right corner of the window.
3. Define the sensitivity to moving objects and the space ratio of all alerted pixels by moving the Sensitivity and Percentage slider bar.
4. Click **Save** to enable the settings.
5. Select **Enable motion detection** to enable this function.

For example:

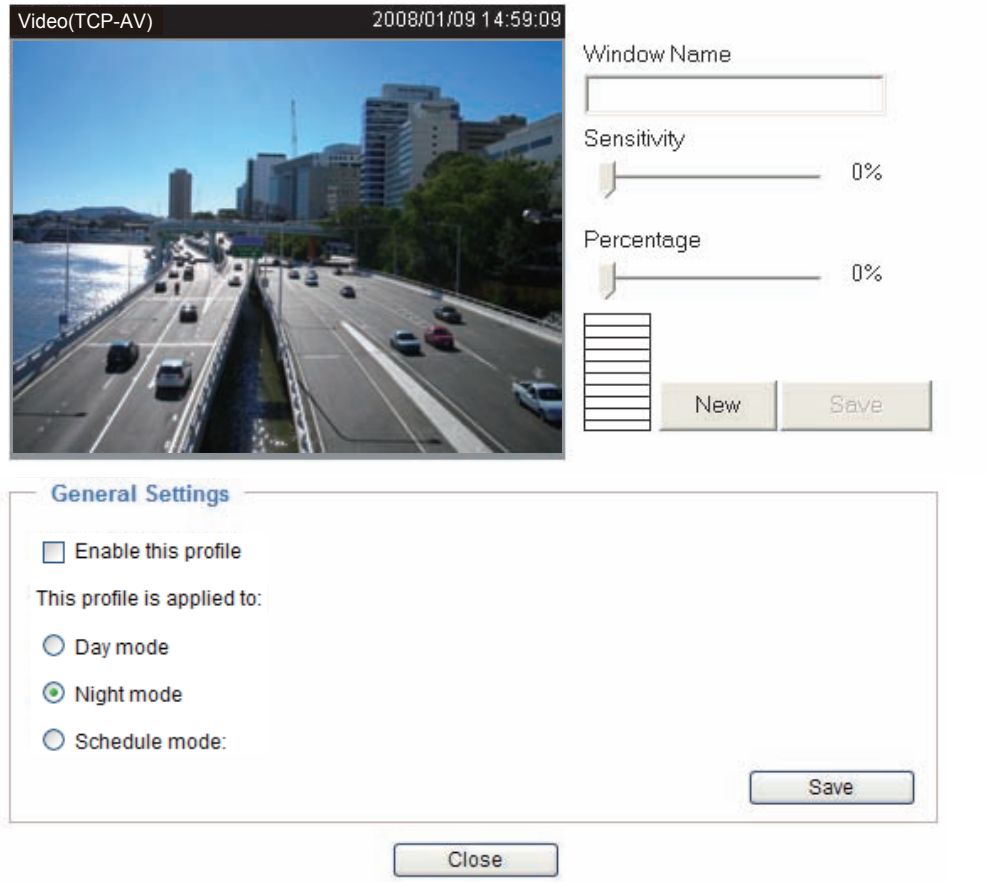


The Percentage Indicator will rise or fall depending on the variation between sequential images. When motions are detected by the Network Camera and are judged to exceed the defined threshold, the red bar rises. Meanwhile, the motion detection window will be outlined in red. Photos or videos can be captured instantly and configured to be sent to a remote server (Email, FTP) by utilizing this feature as a trigger source. For more information on how to set an event, please refer to Application on page 85.

A green bar indicates that even though motions have been detected, the event has not been triggered because the image variations still fall under the defined threshold.



If you want to configure other motion detection settings for day/night/schedule mode, please click **Profile** to open the Motion Detection Profile Settings page as shown below. A total of three motion detection windows can be configured on this page as well.

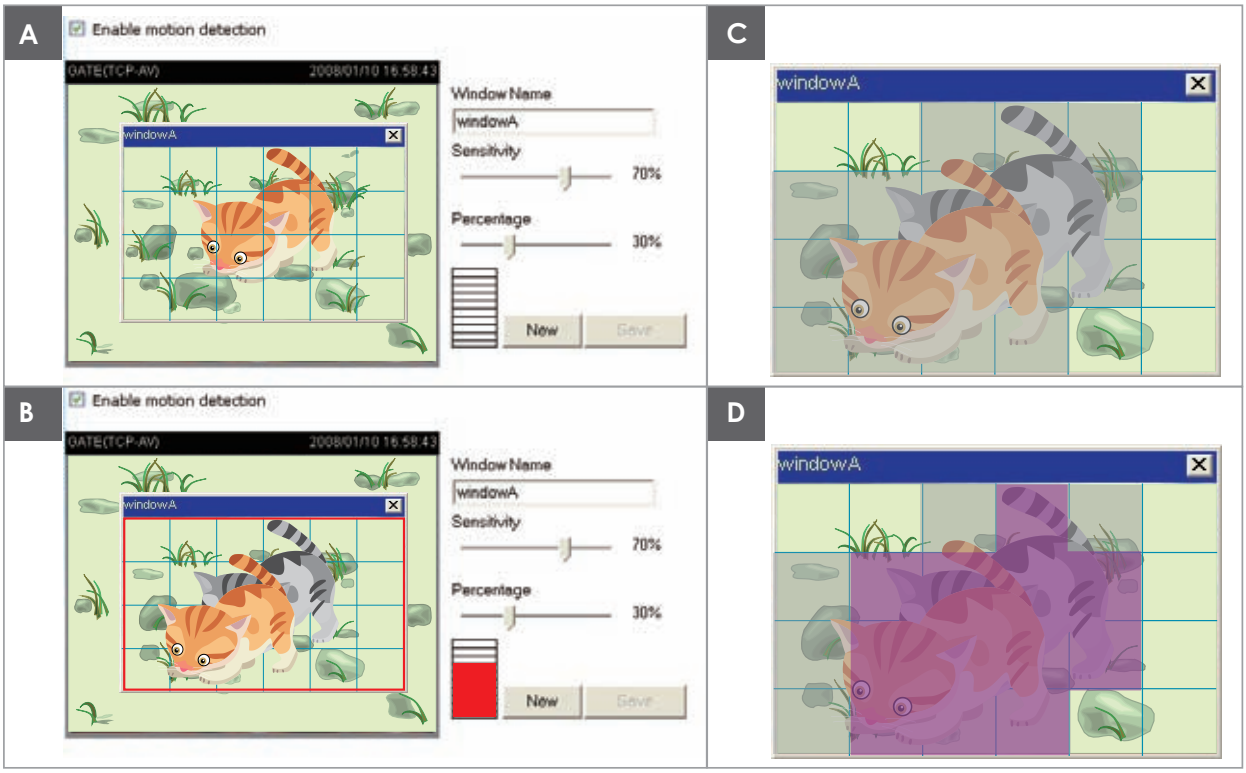


Please follow the steps beolw to set up a profile:
1. Create a new motion detection window.
2. Check **Enable this profile**.
3. Select the applicable mode: Day mode, Night mode, or Schedule mode. Please manually enter a time range if you choose Schedule mode.
4. Click **Save** to enable the settings and click **Close** to exit the page.

This motion detection window will also be displayed on the Event Settings page. You can go to Application > Event Settings > Trigger to choose it as a trigger source. Please refer to page 87 for detailed information.

NOTE

► *How does motion detection work?*



There are two motion detection parameters: Sensitivity and Percentage. In the illustration above, frame A and frame B are two sequential images. Pixel differences between the two frames are detected and highlighted in gray (frame C) and will be compared with the sensitivity setting. Sensitivity is a value that expresses the sensitivity to moving objects. Higher sensitivity settings are expected to detect slight movements while smaller sensitivity settings will neglect them. When the sensitivity is set to 70%, the Network Camera defines the pixels in the purple areas as "alerted pixels" (frame D).

Percentage is a value that expresses the proportion of "alerted pixels" to all pixels in the motion detection window. In this case, 50% of pixels are identified as "alerted pixels". When the percentage is set to 30%, the motions are judged to exceed the defined threshold; therefore, the motion window will be outlined in red.

For applications that require a high level of security management, it is suggested to use higher sensitivity settings and smaller percentage values.

Camera Tampering Detection

This section explains how to set up camera temper detection. With tamper detection, the camera is capable of detecting incidents such as **redirection**, **blocking or defocusing**, or even **spray paint**.

Please follow the steps below to set up the camera tamper detection function:

1. Check **Enable camera tampering detection**.
2. Enter the tamper trigger duration. (10 sec. ~ 10 min.) The tamper alarm will be triggered only when the tampering factor (the difference between current frame and pre-saved background) exceeds the trigger threshold.
3. Set up the event source as Camera Tampering Detection on **Application page** > **Event Settings / Server Settings (how to send alarm message) / Media Settings (send what type of alarm message)**. Please refer to page 87 for detailed information.

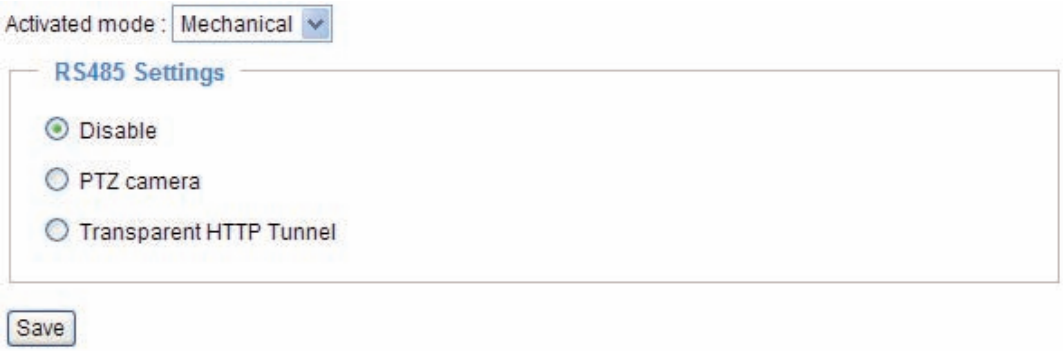
Camera Control

This section explains how to control the Network Camera's Pan/Tilt/Zoom operation.
There are two ways to enable the camera control function:

1. Mechanical: Connect the Network Camera to a PTZ driver or scanner via RS485 interface.
2. Digital: Control the e-PTZ operation. It allows users to quickly move the focus to a target area for close-up viewing without moving the camera physically. Please refer to page 80 for detailed instruction.

Mechanical PTZ Operation

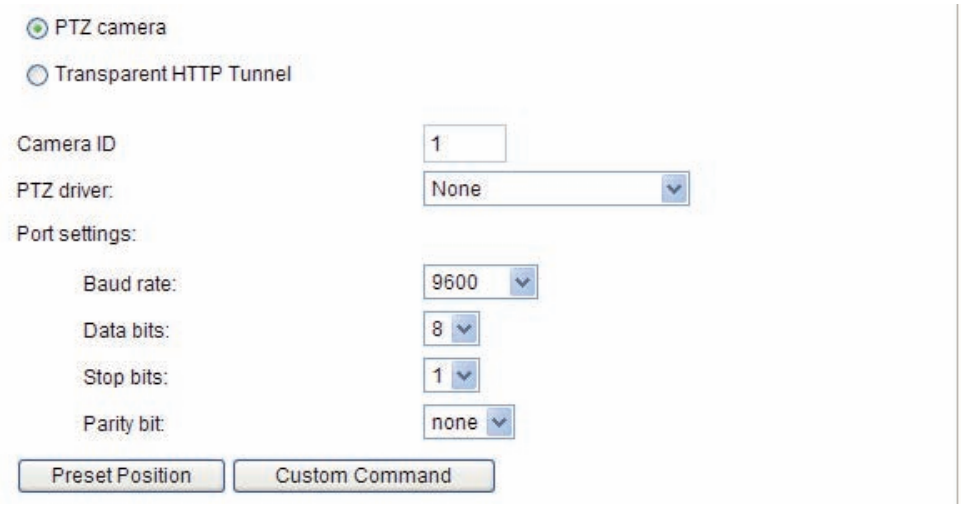
If you select "Mechanical", the RS485 Settings section will be displayed as shown below:



RS485 Settings

Disable: Select this option to disable this function.

PTZ camera: Select this option to enable PTZ operation.
To utilize this feature, please connect the Network Camera to a PTZ driver or scanner via RS485 interface first. Then you can configure the PTZ driver and RS485 port with the following settings.



VIVOTEK offers three PTZ drivers: DynaDome/SmartDOME, Lilin PIH-7x00, and Pelco D protocol. If none of the above PTZ drivers is supported by your PTZ scanner, please select **Custom camera** (scanner). Please refer to the user's manual of your PTZ scanner to determine the Camera ID, PTZ driver, and Port settings. The Camera ID is necessary to control multiple cameras. If you click **Save** to enable this function, the camera control panel will be displayed on the main page. Please refer to the illustration on page 77.

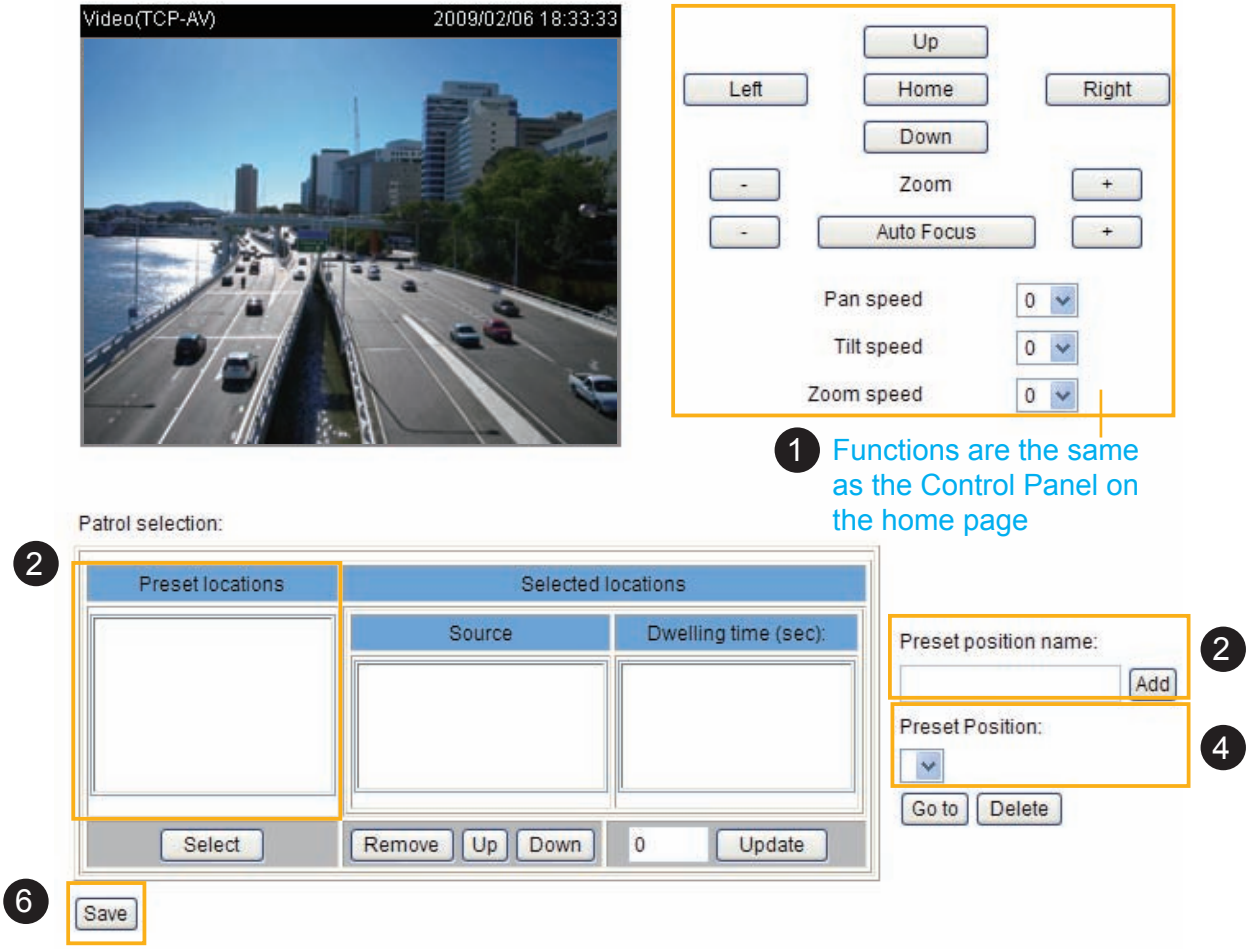
Transparent HTTP Tunnel: If you want to use your own RS-485 device, you can use UART commands to build a Transparent HTTP Tunnel. The UART commands will be sent through HTTP tunnel established between the RS-485 device and the linked camera. For detailed application notes, please refer to URL Commands on page 111 or http://www.vivotek.com/downloadfiles/faq/videoserver/UART_HTTP_Tunnel.pdf.

Preset Positions

If you select DynaDome/SmartDOME, Lilin PIH-7x00, or Pelco D protocol as the PTZ driver and click the **Save** button, the **Preset Position** button will be enabled. Click **Preset Position** to open the settings page. You can also select preset positions for the camera to patrol. A total of 20 preset positions can be configured.

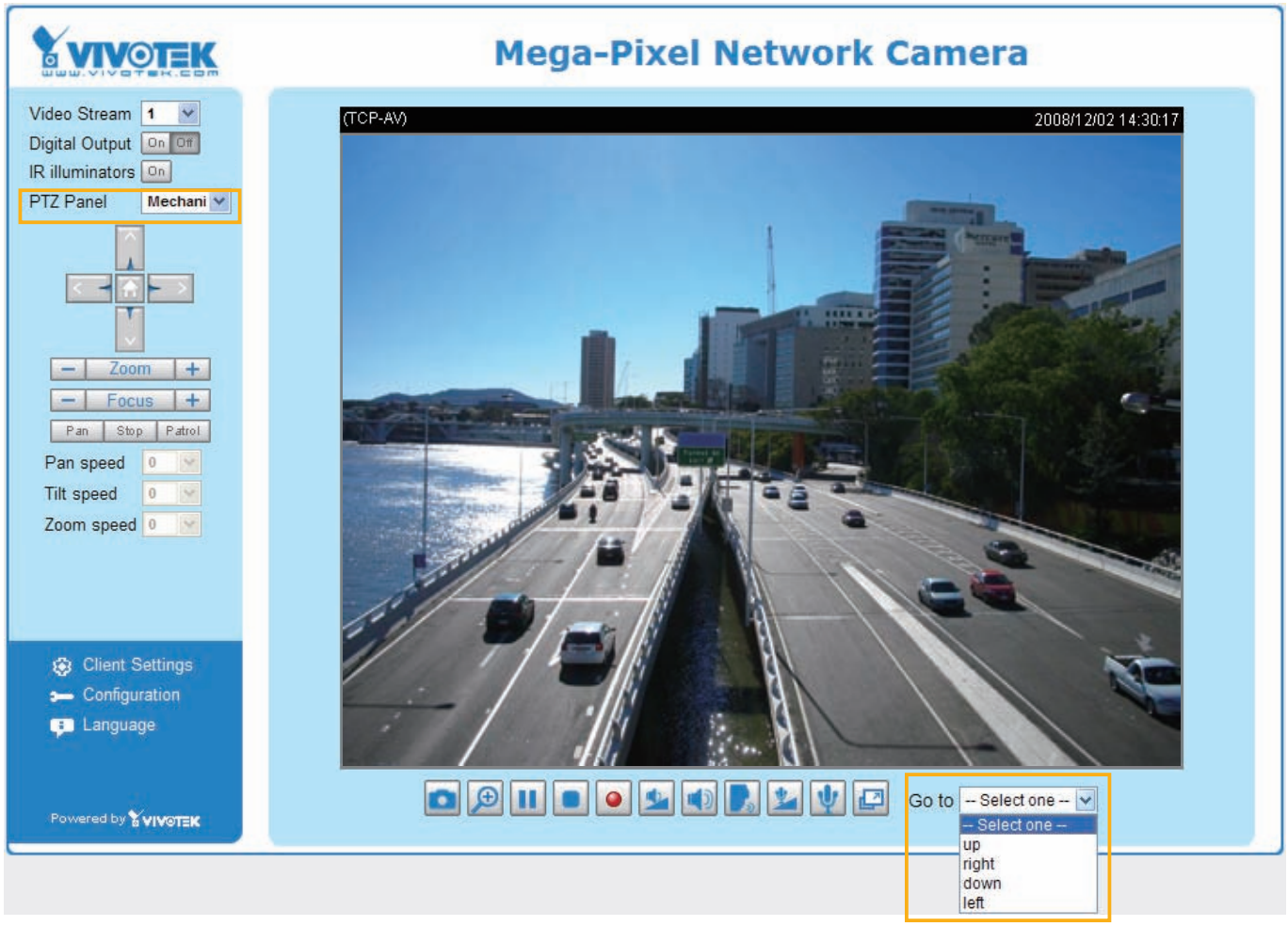
Please follow the steps below to preset a position:

1. Adjust the shooting area to the desired position using the buttons on the right side of the window.
2. Enter a name for the preset position, which allows for up to forty characters. Click **Add** to enable the settings. The preset positions will be displayed under the Preset Location list on the left-hand side.
3. To add additional preset positions, please repeat steps 1~2.
4. To remove a preset position from the list, select it from the drop-down list and click **Delete**.
5. The preset positions will also displayed on the main page. Please refer to the illustration on the next page.
6. Click **Save** to enable the settings.



Home page in Mechanical PTZ Mode

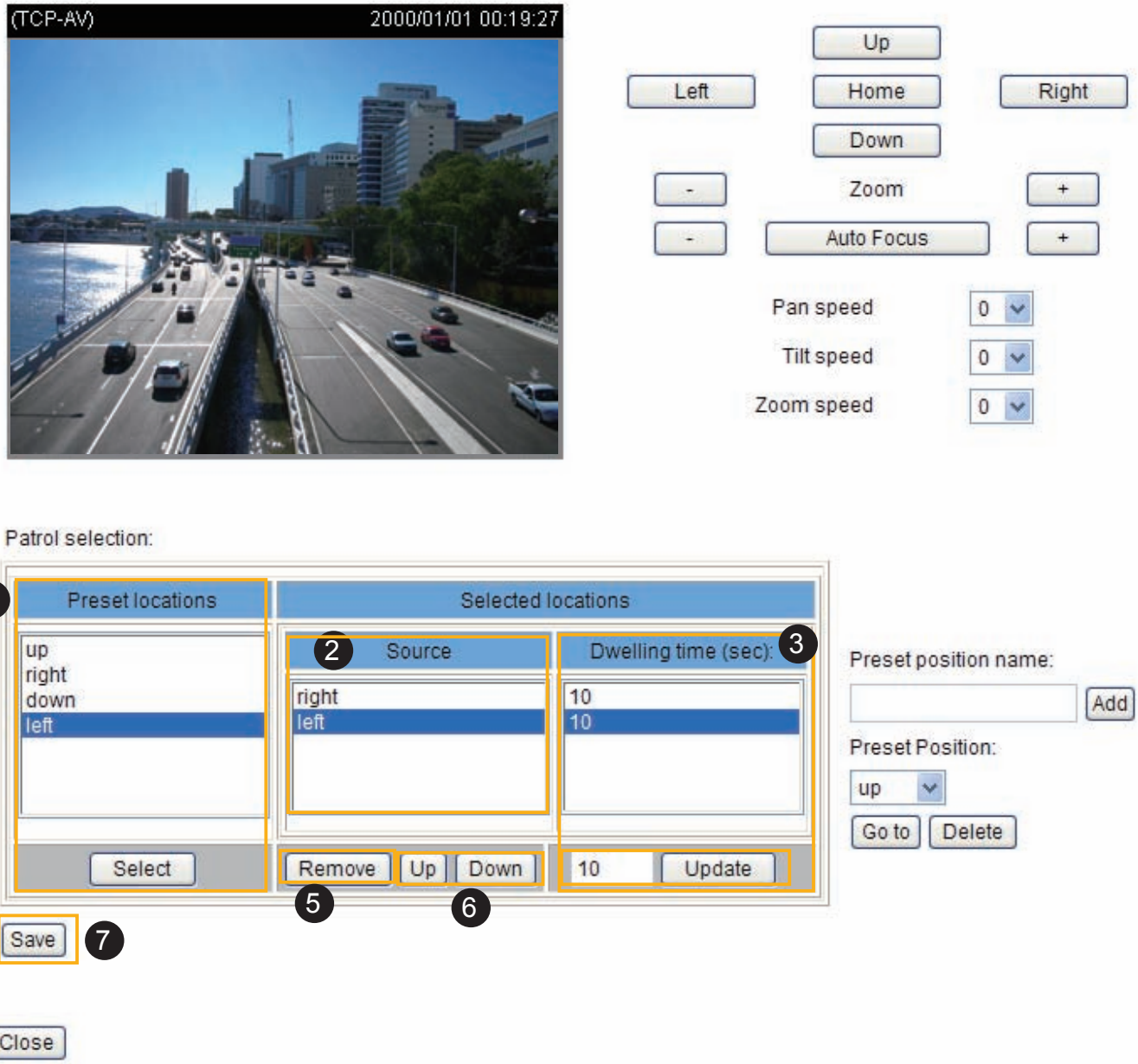
The Preset Positions will also be displayed on the home page. Select one from the drop-down list, and the Network Camera will move to the selected preset position.



Patrol Settings

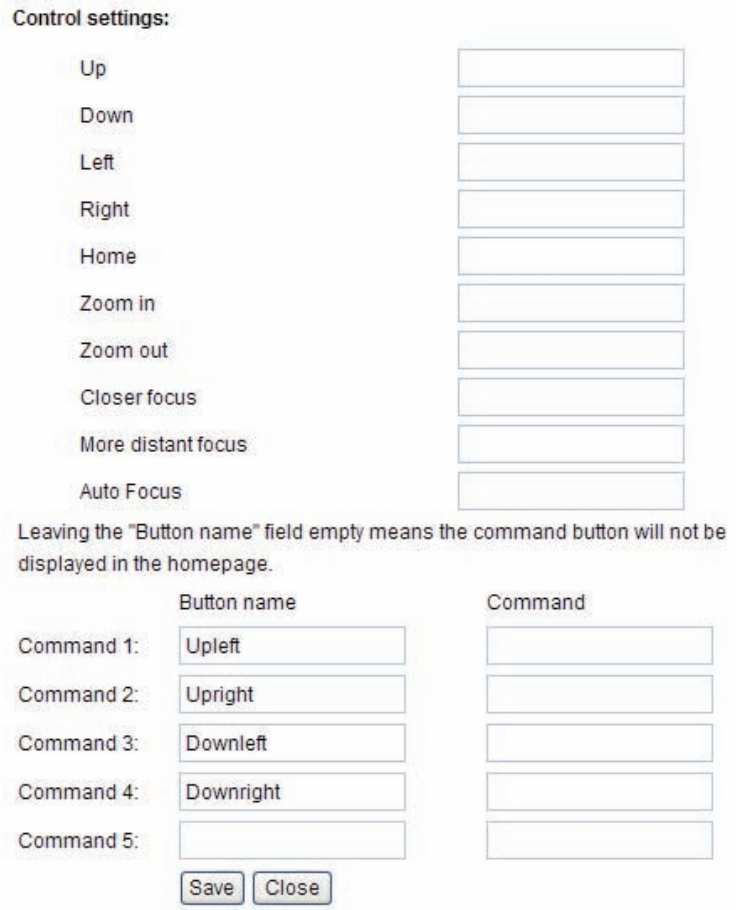
You can select some preset positions for the Network Camera to patrol.
Please follow the steps below to set up a patrol schedule:

1. Click a preset location on the list and click **Select**.
2. The selected preset location will be displayed on the **Source** list.
3. Set the **Dwelling time** for the preset location during auto patrol. You can also manually enter a value in the blank and click **Update**.
4. Repeat step 1 and 3 to select additional preset locations.
5. If you want to delete a selected location, select it from the Source list and click **Remove**.
6. Select a location and click **Up** or **Down** to rearrange the patrol order.
7. Click **Save** to enable the settings.



Custom Command

If **Custom Camera (scanner)** is selected as the PTZ driver, you will need to configure command buttons to control the PTZ scanner. Click **Custom Command** to open the Custom Command page to set the commands in the Control Settings session. Please refer to your PTZ scanner user's manual to enter the commands in the following fields. Click **Save** to enable the settings and click **Close** to exit the page.

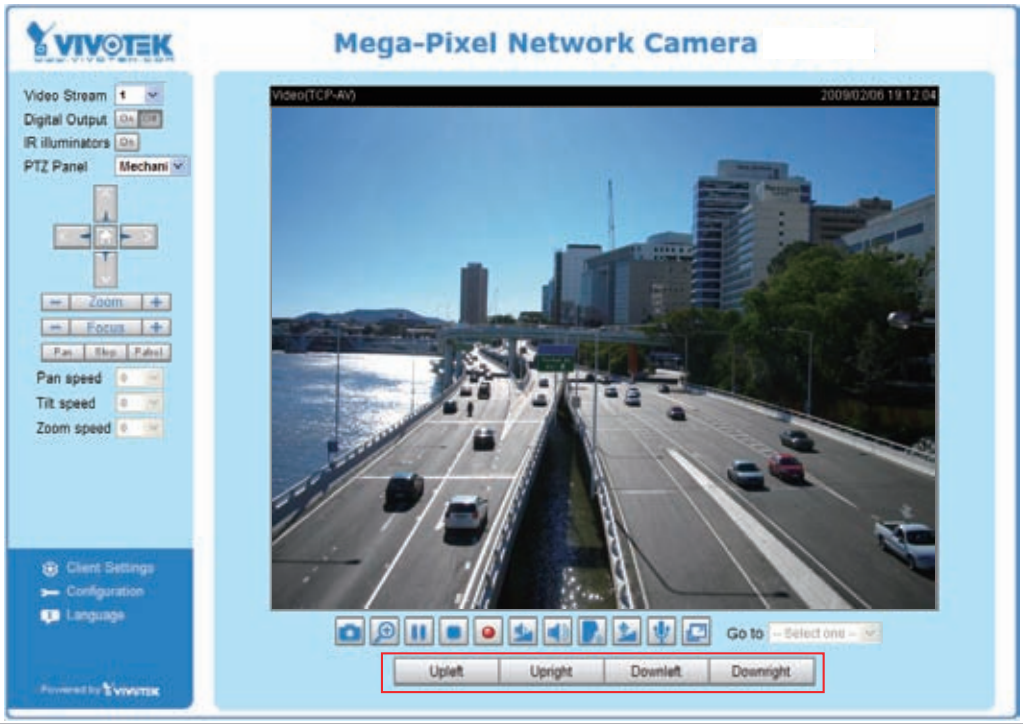


NOTE

►*If you select DynaDome/SmartDOME, Lilin PIH-7x00, or Pelco D protocol as the PTZ driver, the Control Settings column will not be displayed.*

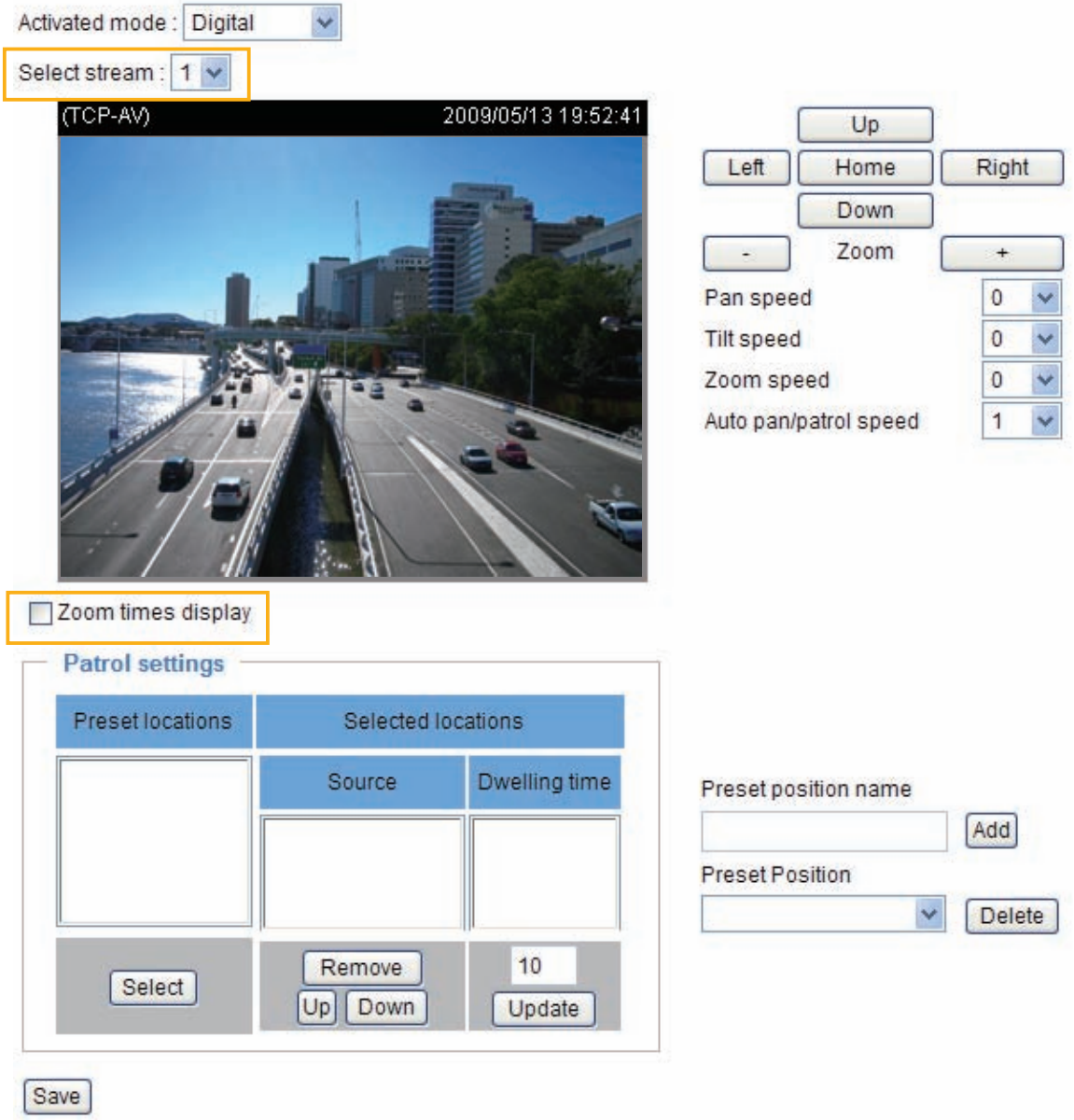
►*For all PTZ drivers, a total of five additional command buttons can be configured.*

►*The command buttons will be displayed on the main page:*



E-PTZ Operation

If you select “Digital“, the e-PTZ control settings section will be displayed as shown below:

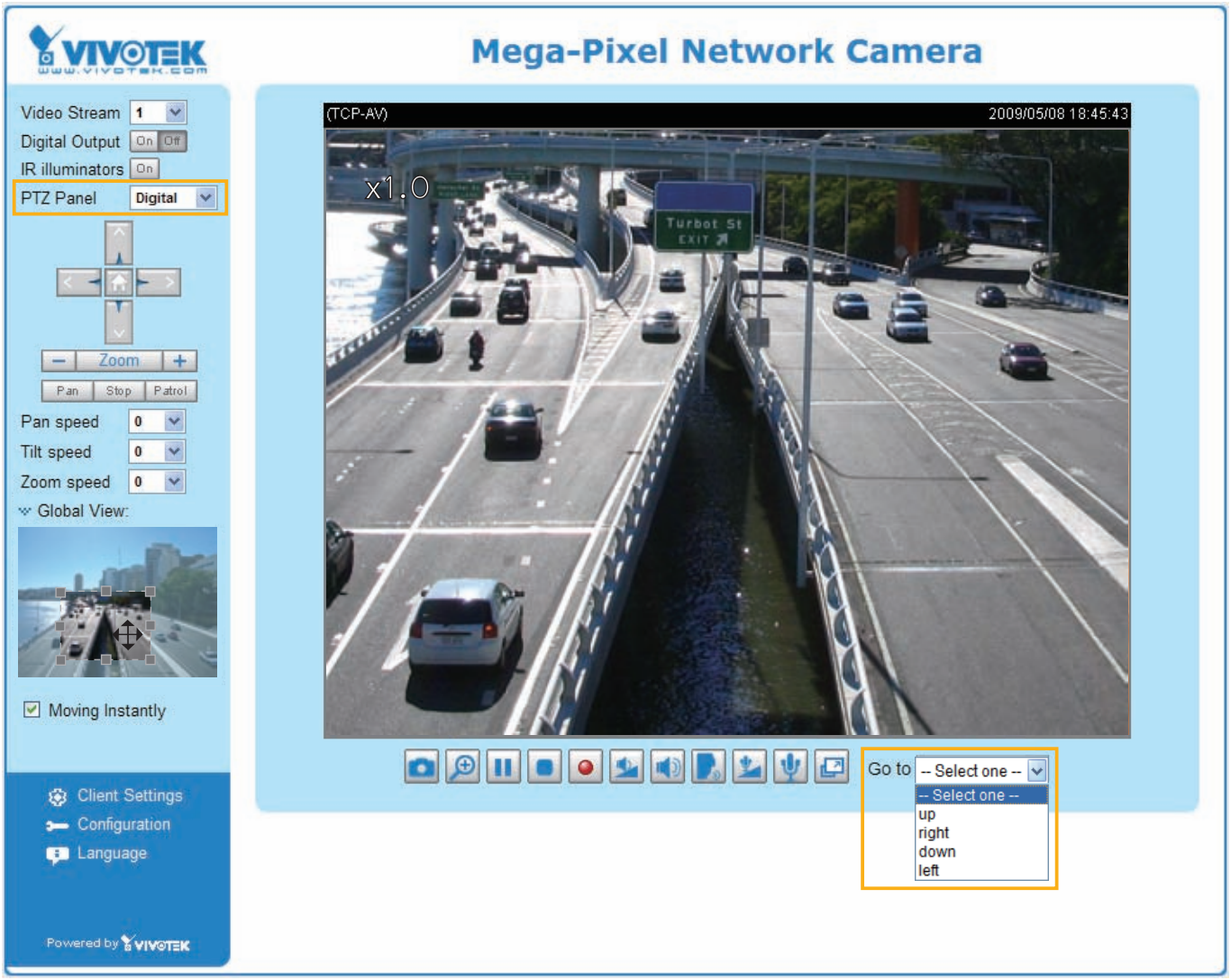


Select Stream: Select one of the stream 1~3 to set up the e-PTZ control. Please note that **each stream can be set up with its own e-preset positions and e-patrol settings**. For detailed information about how to set up **Preset Positions** and **Patrol Settings**, please refer to page 76~78.

Zoom Times Display
If you check this item, the zoom indicator will be displayed on the home page when you zoom in/out the live viewing window as the picture shown on the next page.

When completed with the settings of e-PTZ, click **Save** to enable the settings on this page.

Home page in E-PTZ Mode



- The e-Preset Positions will also be displayed on the home page. Select one from the drop-down list, and the Network Camera will move to the selected e-preset position.
- If you have set up different e-preset positions for stream 1~3, you can select one of the video streams to display its separate e-preset positions.

Global View

In addition to using the e-PTZ control panel, you can also use the mouse to drag or resize the floating frame to pan/tilt/zoom the viewing region. The live view window will also move to the viewing region accordingly.

Moving Instantly

If you check this item, the live view window will switch to the new viewing region instantly after you move the floating frame.

Click on Image

The e-PTZ function also supports “Click on Image“. When you click on any point of the Global View Window or Live View Window, the viewing region will also move to that point.

Homepage Layout Advanced Mode

This section explains how to set up your own customized homepage layout.

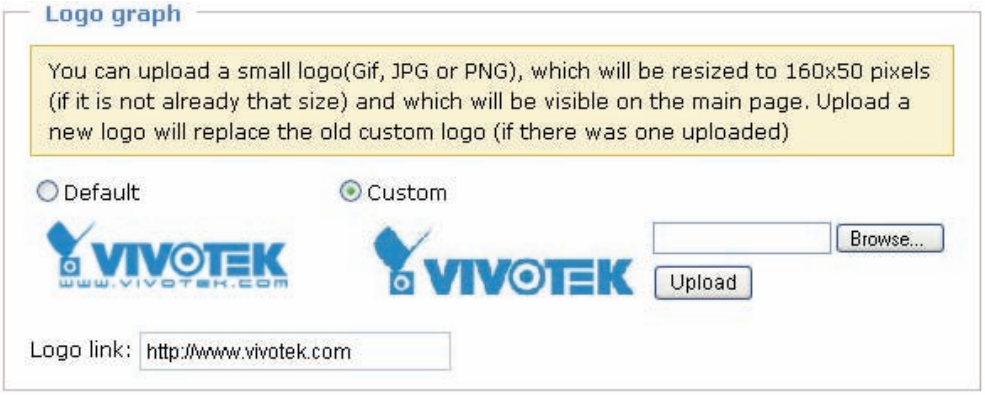
Preview

This column shows the settings of your hompage layout. You can manually select the background and font colors in Theme Options (the third column on this page). The settings will be displayed automatically in this Preview field. The following shows the homepage using the default settings:

■ Hide Powered by VIVOTEK: If you check this item, it will be removed from the homepage.

Logo

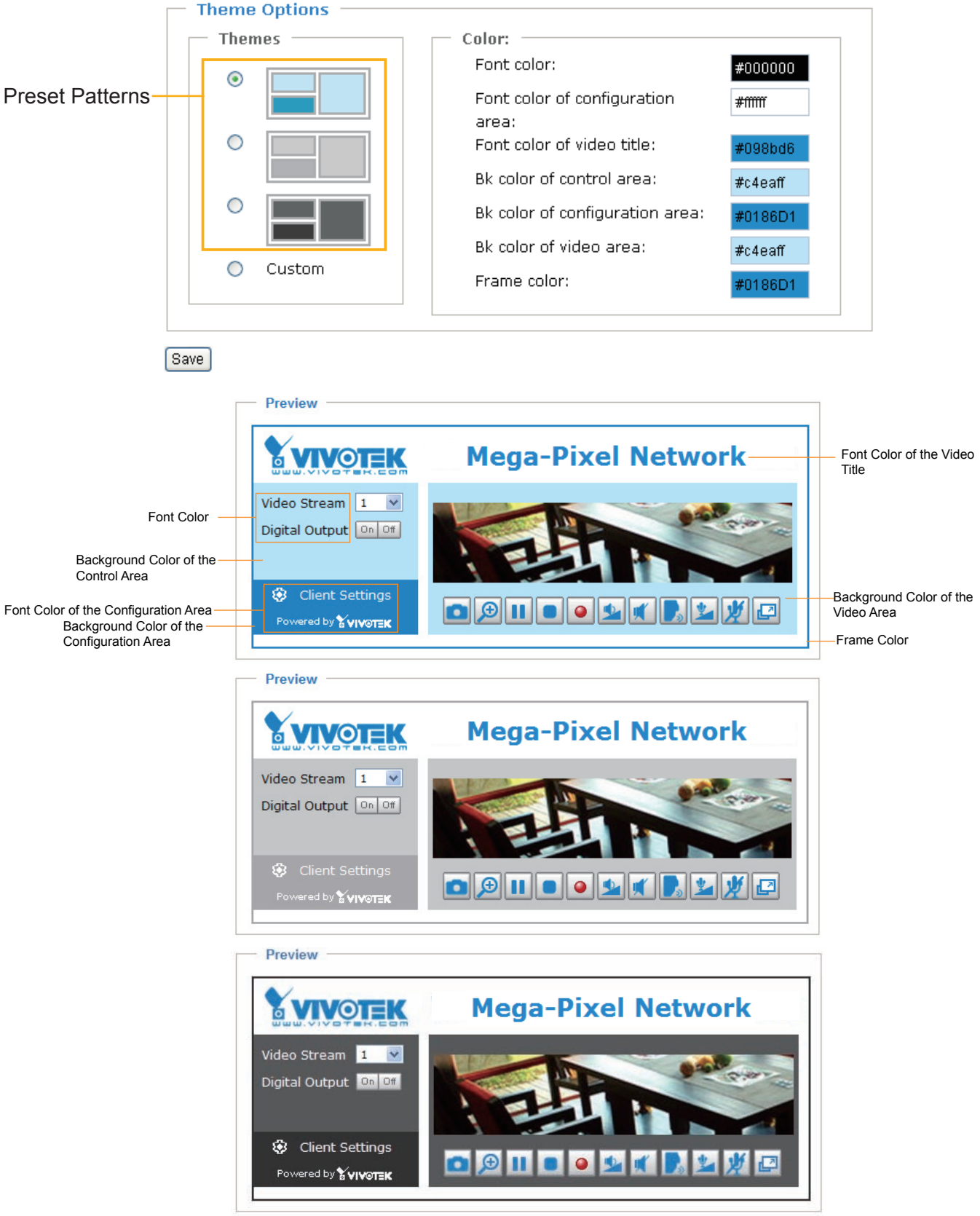
Here you can change the logo at the top of your homepage.



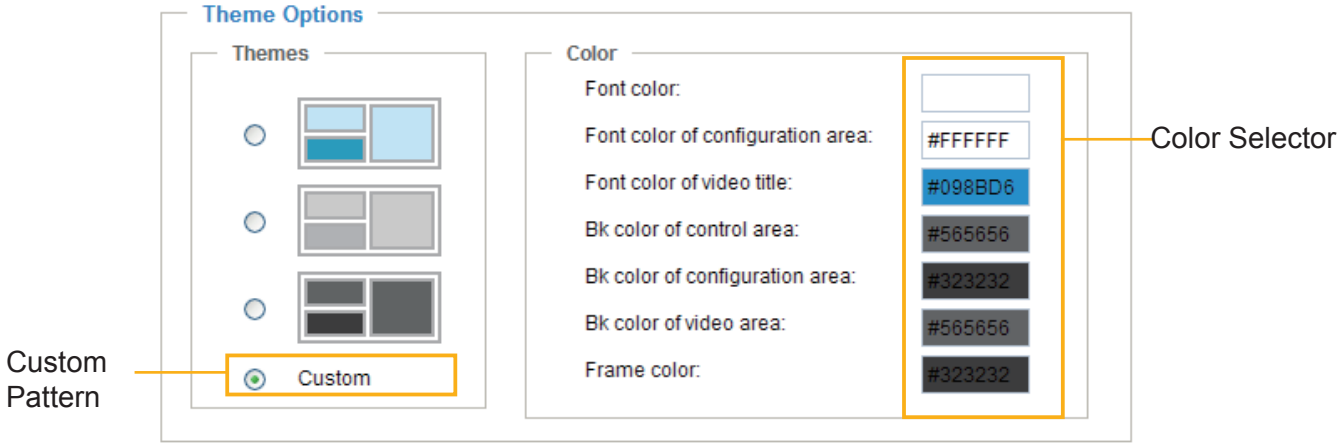
Follow the steps below to upload a new logo:
1. Click **Custom** and the Browse field will appear.
2. Select a logo from your files.
3. Click **Upload** to replace the existing logo with a new one.
4. Enter a website link if necessary.
5. Click **Save** to enable the settings.

Theme Options

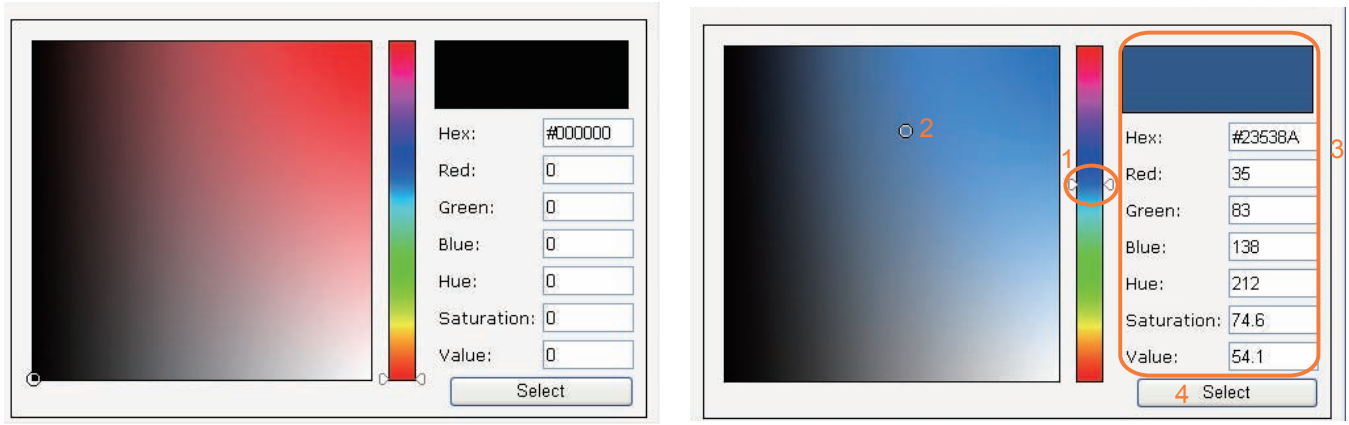
Here you can change the color of your homepage layout. There are three types of preset patterns for you to choose from. The new layout will simultaneously appear in the **Preview** filed. Click **Save** to enable the settings.



■ Follow the steps below to set up the customed homepage:
1. Click **Custom** on the left column.
2. Click the field where you want to change the color on the right column.



3. The palette window will pop up as shown below.

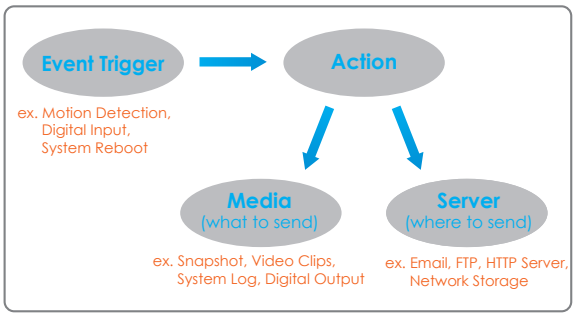


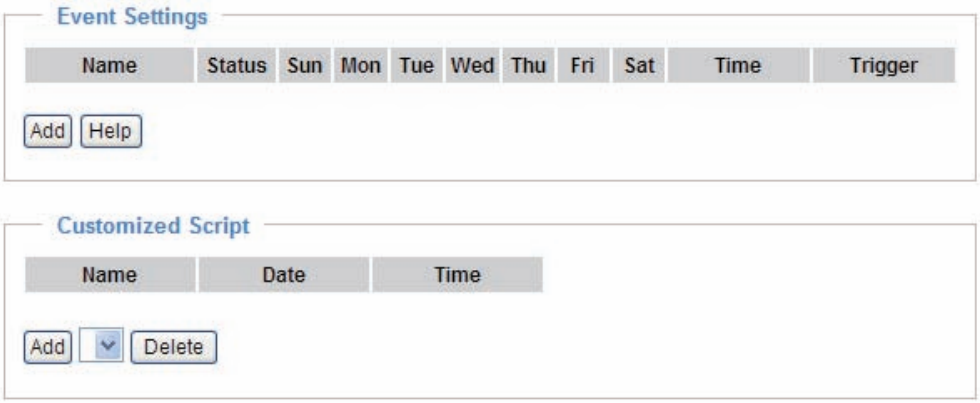
4. Drag the slider bar and click on the left square to select a desired color.
5. The selected color will be displayed in the corresponding fields and in the **Preview** column.
6. Click **Save** to enable the settings.

Application Advanced Mode

This section explains how to configure the Network Camera to responds to particular situations (event). A typical application is that when a motion is detected, the Network Camera sends buffered images to an FTP server or e-mail address as notifications.

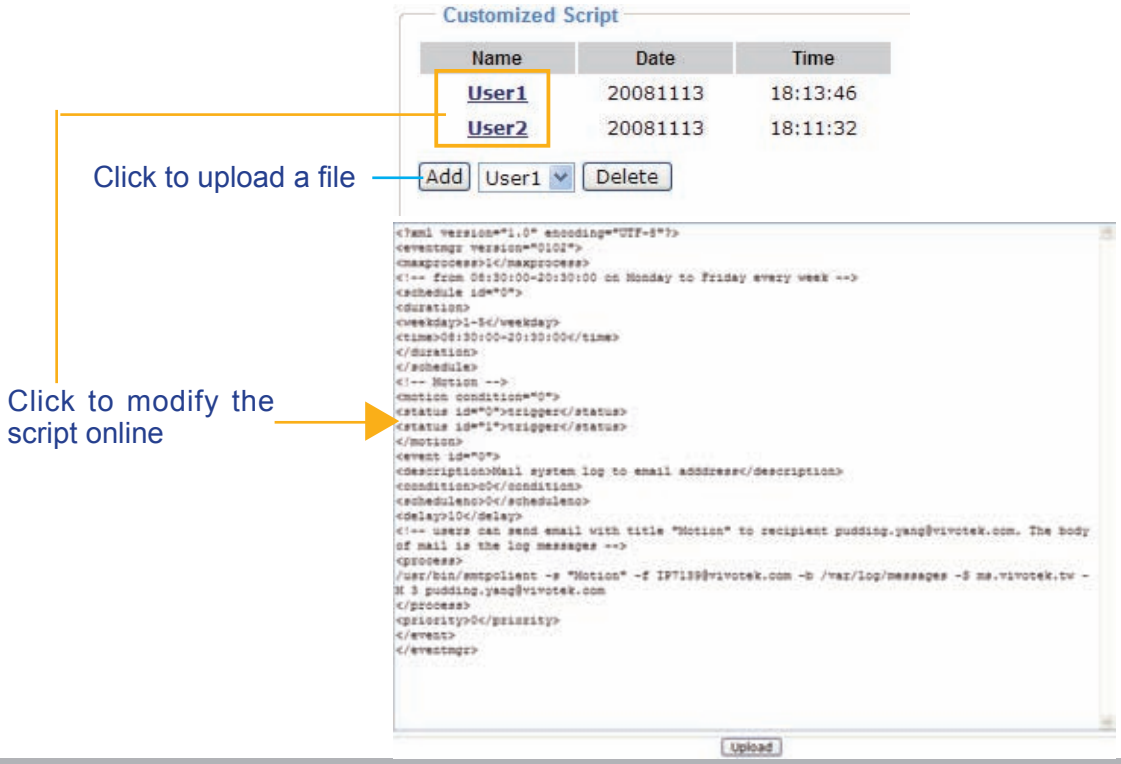
In the illustration on the right, an event can be triggered by many sources, such as motion detection or external digital input devices. When an event is triggered, you can specify what type of action that will be performed. You can configure the Network Camera to send snapshots or videos to your email address or FTP site.





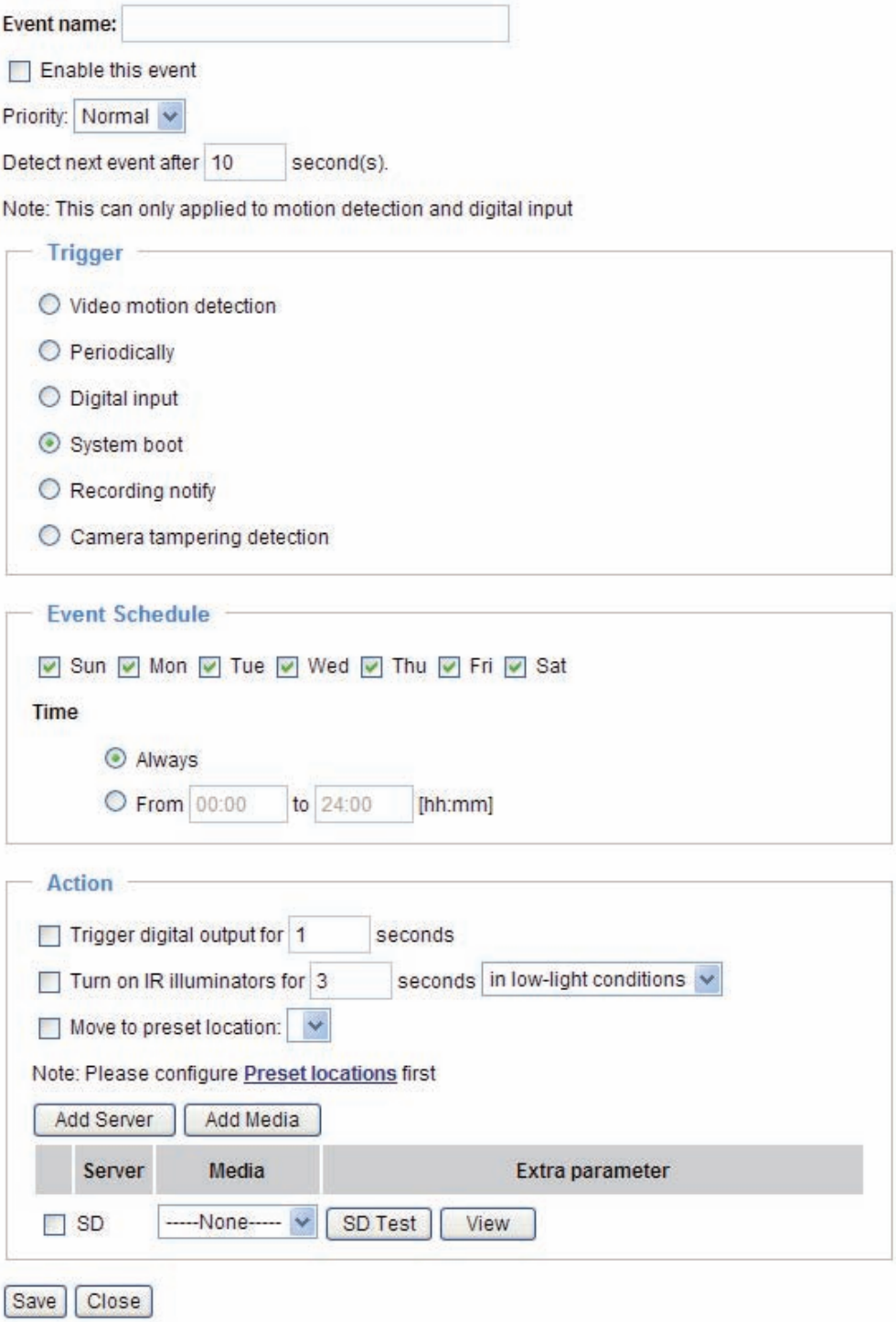
Customized Script

This function allows you to upload a sample script (.xml file) to the webpage, which will save your time on configuring the settings. Please note that there is a limited number of customized scripts you can upload; if the current amount of customized scripts has reached the limit, an alert message will pop up. If you need more information, please ask for VIVOTEK technical support.



Event Settings

In the **Event Settings** column, click **Add** to open the **Event Settings** page. On this page, you can arrange three elements -- Trigger, Schedule, and Action to set an event. A total of 3 event settings can be configured.



Event name: Enter a name for the event setting.

Enable this event: Select this option to enable the event setting.

Priority: Select the relative importance of this event (High, Normal, or Low). Events with a higher priority setting will be executed first.

Detect next event after ☐ seconds: Enter the duration in seconds to pause motion detection after a motion is detected.

An event is an action initiated by a user-defined trigger source; it is the causal arrangement of the following three elements: Trigger, Event Schedule, and Action.

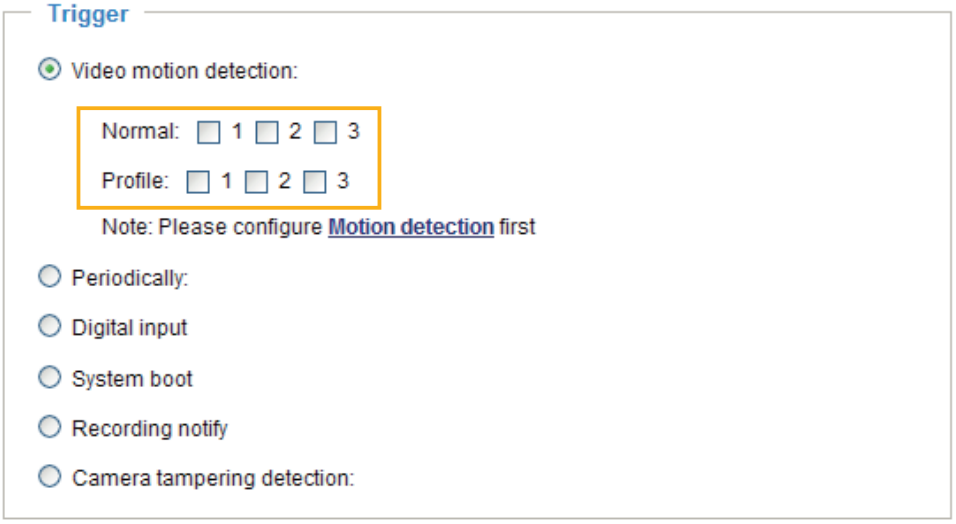
Trigger

This is the cause or stimulus which defines when to trigger the Network Camera. The trigger source can be configured to use the Network Camera's built-in motion detection mechanism or external digital input devices.

There are several choices of trigger sources as shown below. Select the item to display the detailed configuration options.

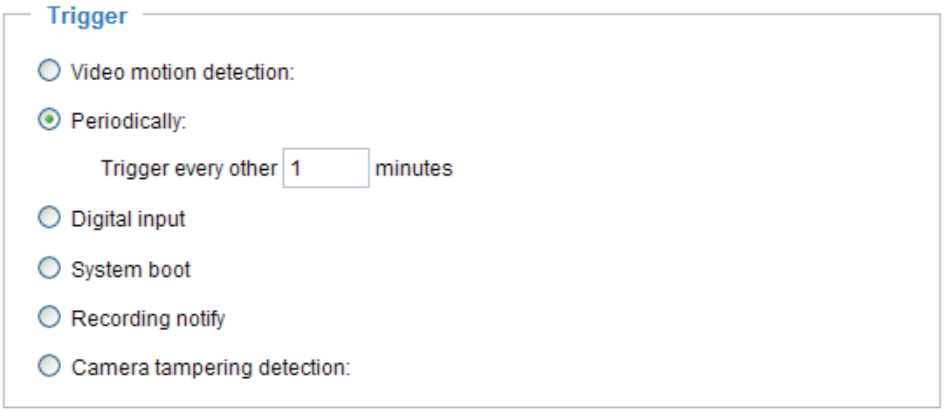
■ Video motion detection

This option makes use of the built-in motion detection mechanism as a trigger source. To enable this function, you need to configure a Motion Detection Window first. For more information, please refer to Motion Detection on page 71 for details.



■ Periodically

This option allows the Network Camera to trigger periodically for every other defined minute. Up to 999 minutes are allowed.



■ Digital input

This option allows the Network Camera to use an external digital input device or sensor as a trigger source. Depending on your application, there are many choices of digital input devices on the market which helps to detect changes in temperature, vibration, sound, and light, etc.

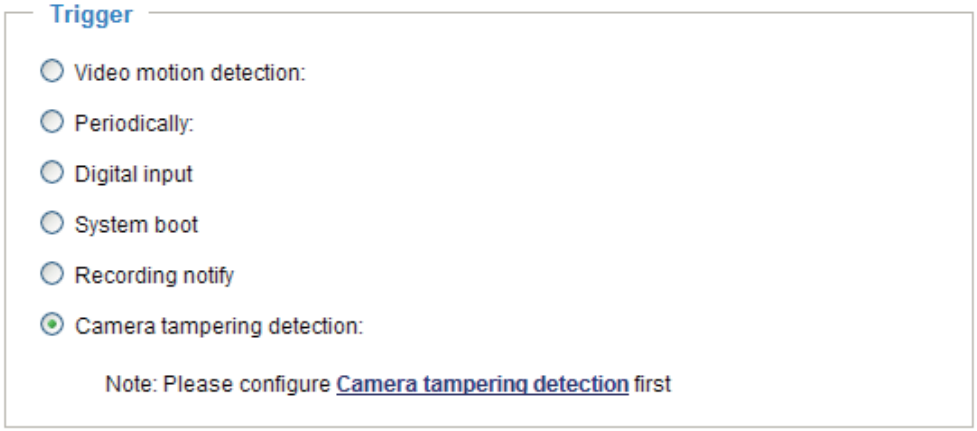
■ System boot

This option triggers the Network Camera when the power to the Network Camera is disconnected.

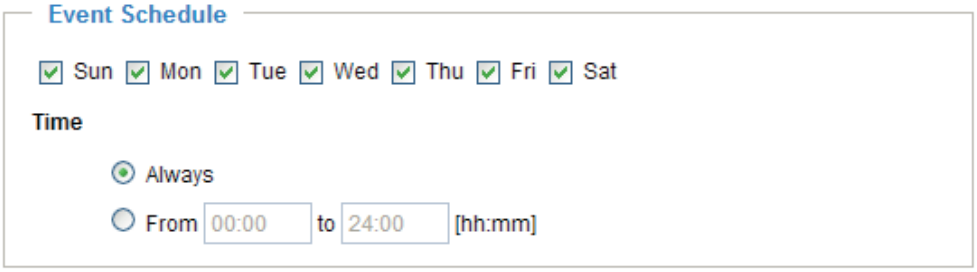
■ Recording notify

This option allows the Network Camera to trigger when the recording disk is full or when recording starts to rewrite older data. If you want receive **Recording notify message**, please refer to page 96 for detailed information.

■ Camera tampering detection
This option allows the Network Camera to trigger when the camera detects that is is being tampered with. To enable this function, you need to configure the Tampering Detection option first. Please refer to page 74 for detailed information.



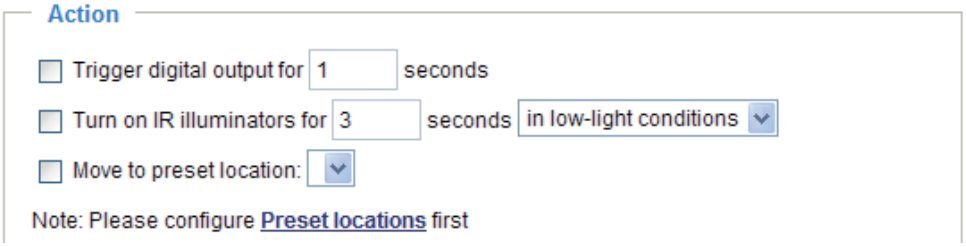
Event Schedule
Specify the period for the event.



■ Select the days of the week.

■ Select the recording schedule in 24-hr time format.

Action
Define the actions to be performed by the Network Camera when a trigger is activated.



■ Trigger digital output for ☐ seconds
Select this option to turn on the external digital output device when a trigger is activated. Specify the length of the trigger interval in the text box.

■ Turn on IR illuminators for ☐ seconds
Select this to turn on IR Illuminators when a trigger is activated every time or only in low light conditions. Specify the length of trigger interval in the text box.

■ Move to preset location: ☐
Select this option, the Network Camera will move to the preset location when a trigger is activated. **This function is only for Mechanical PTZ controlled via RS485 device.** If you do not enable RS485 settings, this item will not appear in this column. Please refer to Camera Control on page 75 for detailed information.

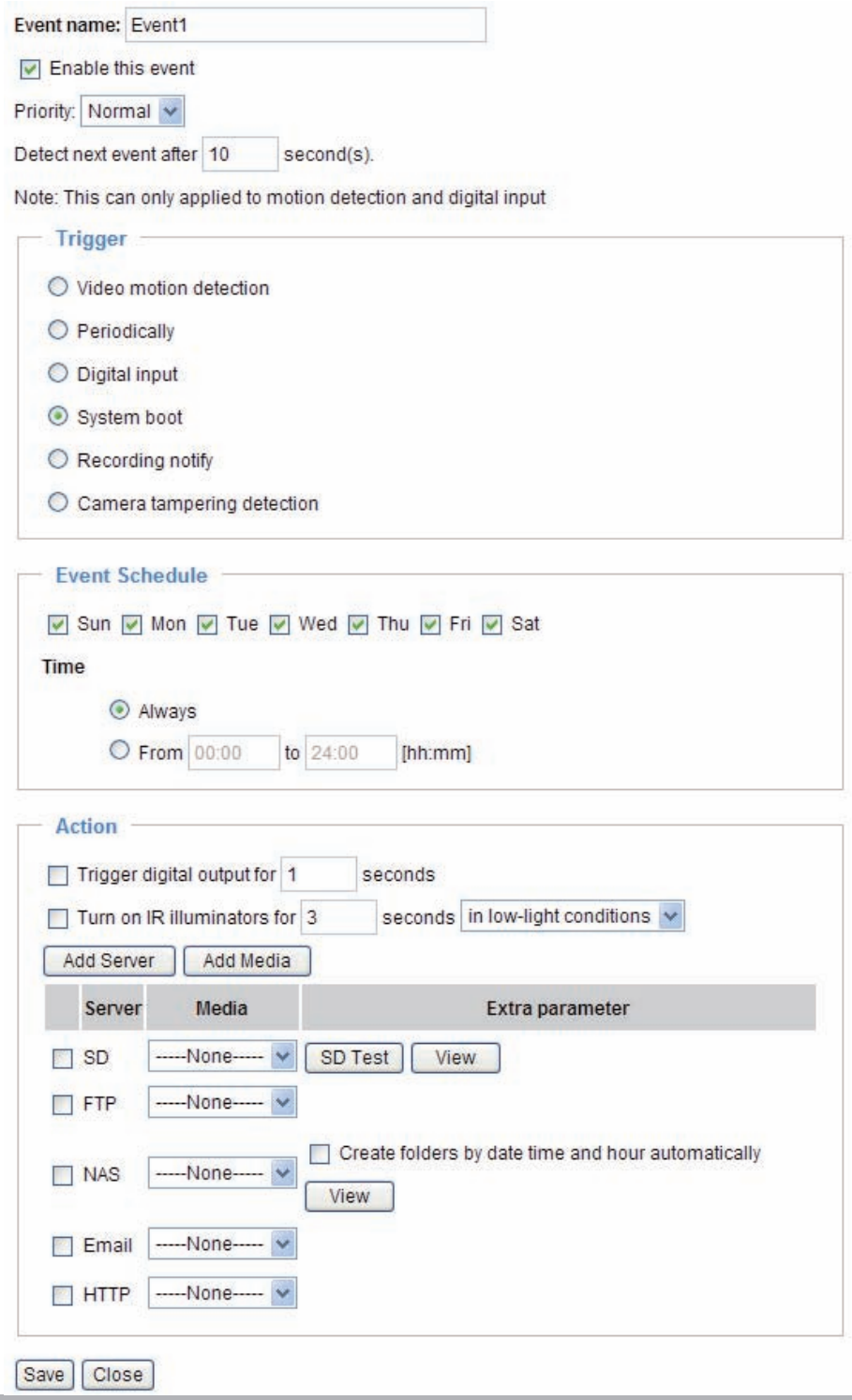
To set an event with recorded video or snapshots, it is necessary to configure the server and media settings so that the Network Camera will know what action to take (such as which server to send the media files to) when a trigger is activated.

■ Add Server / Add Media

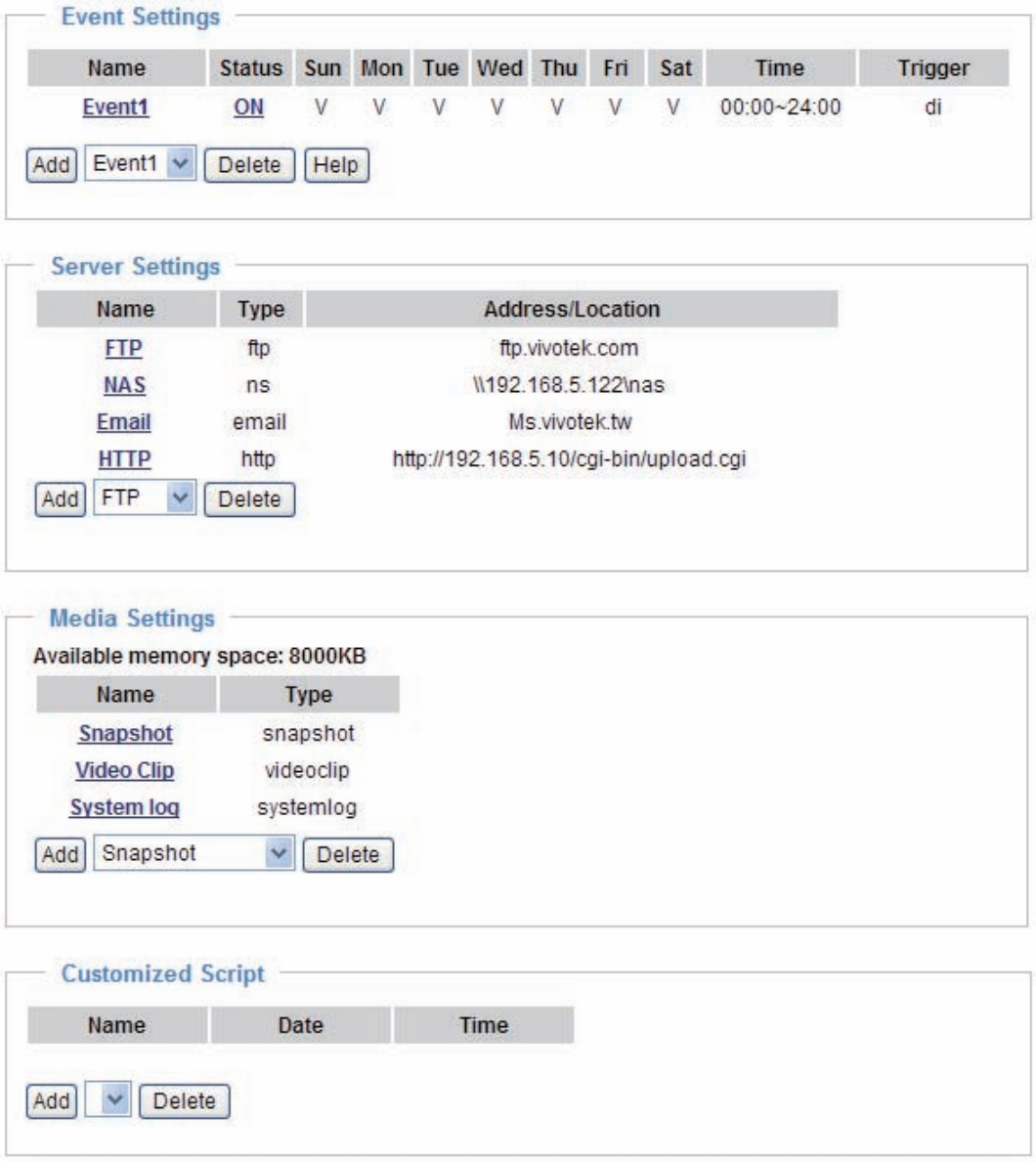
Click **Add Server** to configure Server Settings. For more information, please refer to Server Settings on page 91.

Click **Add Media** to configure Media Settings. For more information, please refer to Media Settings on page 94.

Here is an example of the Event Settings page:



When completed, click **Save** to enable the settings and click **Close** to exit Event Settings page. The new event settings / server settings / media settings will appear in the event drop-down list on the Application page.
Here is an example of the Application page with an event setting:



When the Event Status is **ON**, once an event is triggered by motion detection, the Network Camera will automatically send snapshots via e-mail.

If you want to stop the event trigger, you can click **ON** to turn it to **OFF** status or click **Delete** to remove the event setting.

To remove a server setting from the list, select a server name from the drop-down list and click **Delete**. Note that only when the server setting is not being applied to an event setting can it be deleted.

To remove a media setting from the list, select a media name from the drop-down list and click **Delete**. Note that only when the media setting is not being applied to an event setting can it be deleted.

Server Settings

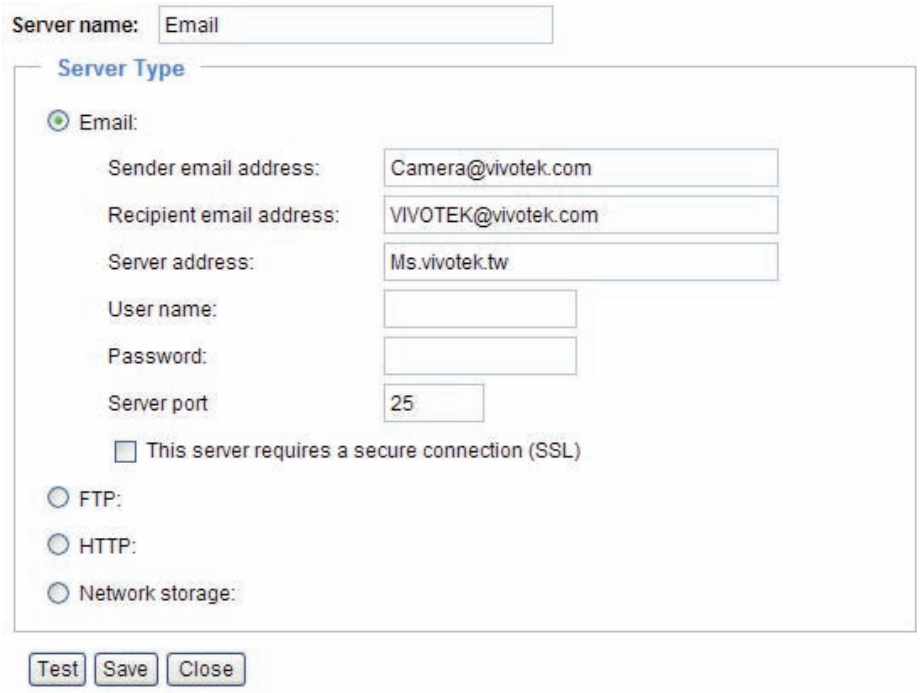
Click **Add Server** on Event Settings page to open the Server Setting page. On this page, you can specify where the notification messages are sent when a trigger is activated. A total of 5 server settings can be configured.

Server name: Enter a name for the server setting.

Server Type

There are four choices of server types available: Email, FTP, HTTP, and Network storage. Select the item to display the detailed configuration options. You can configure either one or all of them.

Email: Select to send the media files via email when a trigger is activated.



■ Sender email address: Enter the email address of the sender.

■ Recipient email address: Enter the email address of the recipient.

■ Server address: Enter the domain name or IP address of the email server.

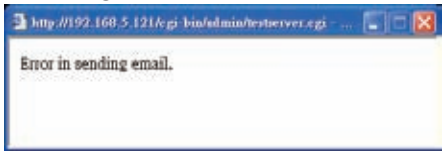
■ User name: Enter the user name of the email account if necessary.

■ Password: Enter the password of the email account if necessary.

■ Server port: The default mail server port is set to 25. You can also manually set another port.

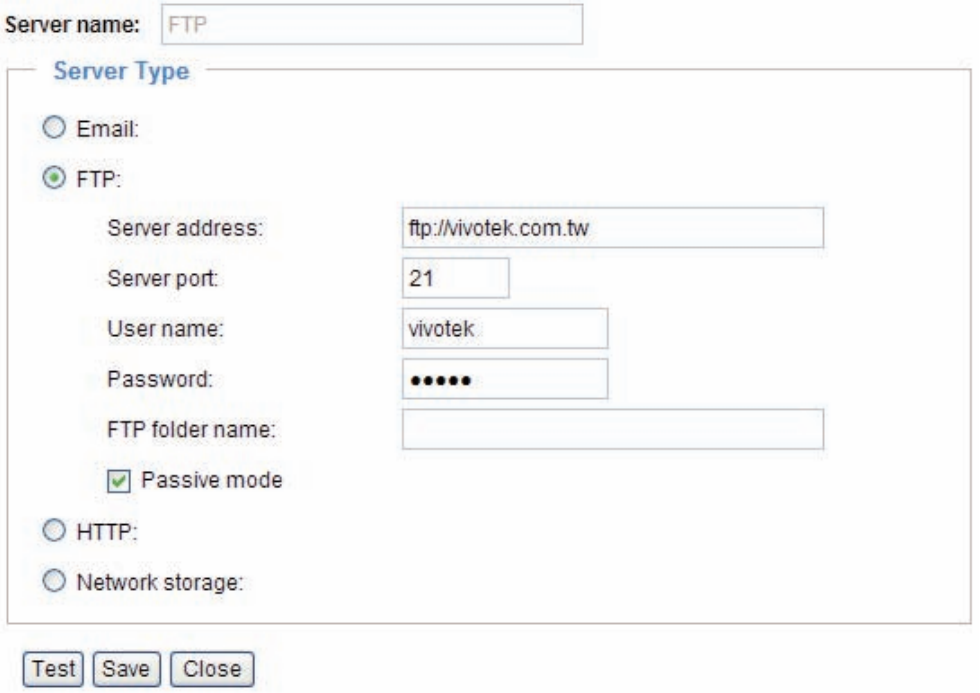
If your SMTP server requires a secure connection (SSL), check **This server requires a secure connection (SSL).**

To verify if the email settings are correctly configured, click **Test**. The result will be shown in a pop-up window. If successful, you will also receive an email indicating the result.



Click **Save** to enable the settings, then click **Close** to exit the page.

FTP: Select to send the media files to an FTP server when a trigger is activated.



■ Server address: Enter the domain name or IP address of the FTP server.

■ Server port
By default, the FTP server port is set to 21. It can also be assigned to another port number between 1025 and 65535.

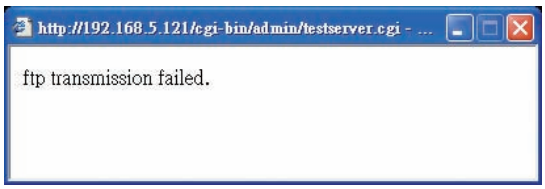
■ User name: Enter the login name of the FTP account.

■ Password: Enter the password of the FTP account.

■ FTP folder name
Enter the folder where the media file will be placed. If the folder name does not exist, the Network Camera will create one on the FTP server.

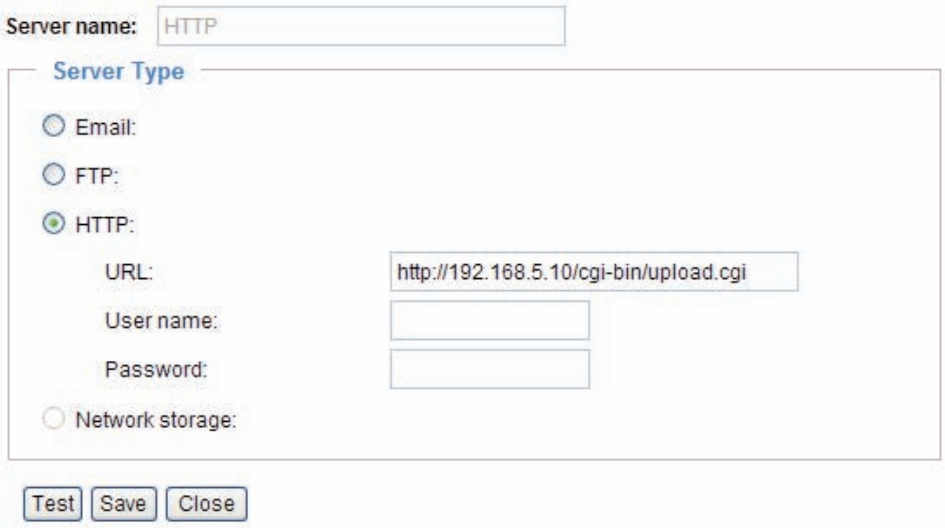
■ Passive mode
Most firewalls do not accept new connections initiated from external requests. If the FTP server supports passive mode, select this option to enable passive mode FTP and allow data transmission to pass through the firewall.

To verify if the FTP settings are correctly configured, click **Test**. The result will be shown in a pop-up window as shown below. If successful, you will also receive a test.txt file on the FTP server.



Click **Save** to enable the settings, then click **Close** to exit the page.

HTTP: Select to send the media files to an HTTP server when a trigger is activated.

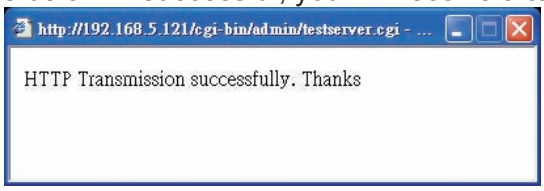


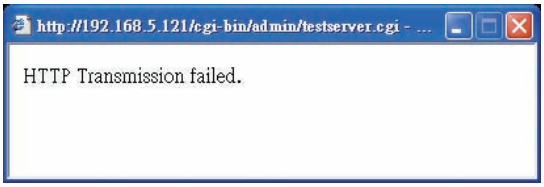
■ URL: Enter the URL of the HTTP server.

■ User name: Enter the user name if necessary.

■ Password: Enter the password if necessary.

To verify if the HTTP settings are correctly configured, click **Test**. The result will be shown in a pop-up window as below. If successful, you will receive a test.txt file on the HTTP server.



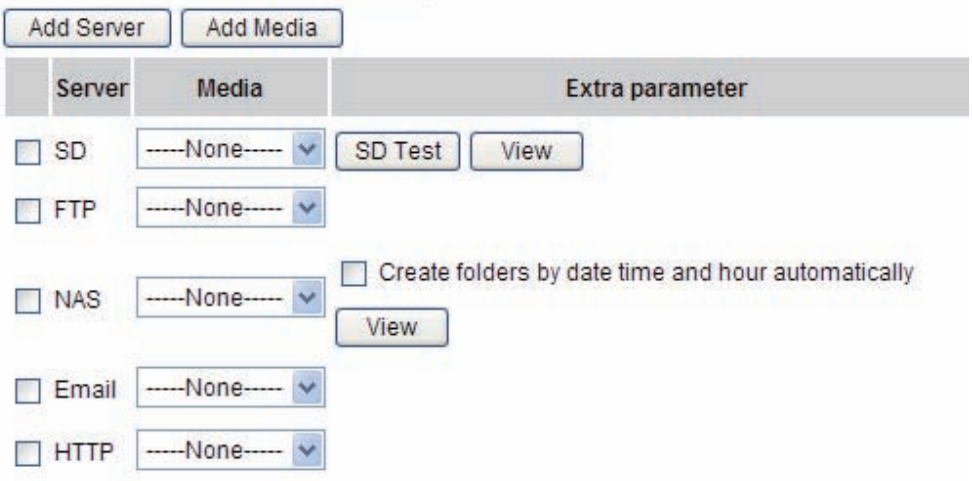


Click **Save** to enable the settings, then click **Close** to exit the page.

Network storage: Select to send the media files to a network storage location when a trigger is activated. Please refer to **Network Storage Setting** on page 98 for details.

Click **Save** to enable the settings, then click **Close** to exit the page.

When completed, the new server settings will automatically be displayed on the Event Settings page. For example:



Media Settings

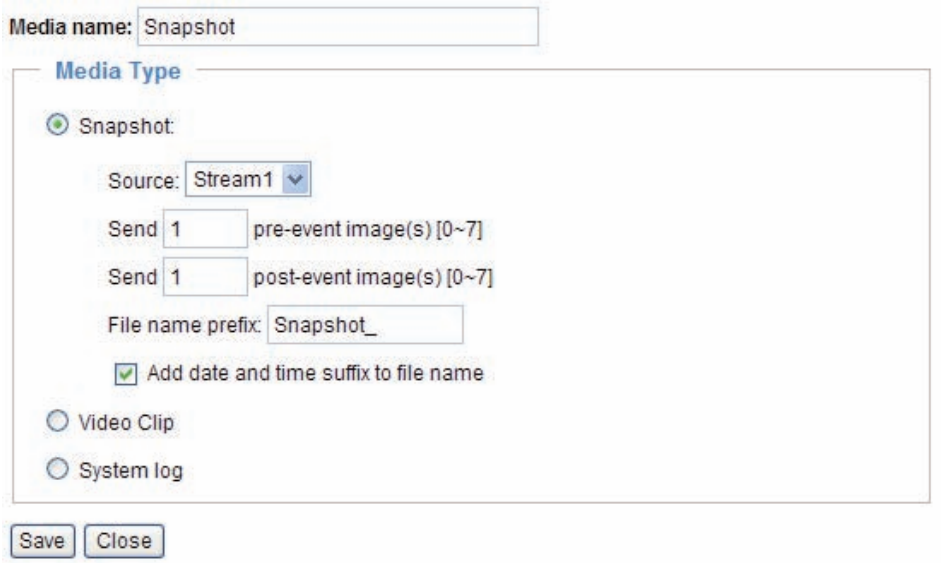
Click **Add Media** on the Event Settings page to open the Media Settings page. On this page, you can specify the type of media that will be sent when a trigger is activated. A total of 5 media settings can be configured.

Media name: Enter a name for the media setting.

Media Type

There are three choices of media types available: Snapshot, Video Clip, and System log. Select the item to display the detailed configuration options. You can configure either one or all of them.

Snapshot: Select to send snapshots when a trigger is activated.

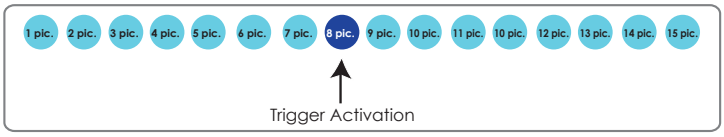


■ Source: Select to take snapshots from stream 1 ~ 4.

■ Send ☐ pre-event images
The Network Camera has a buffer area; it temporarily holds data up to a certain limit. Enter a number to decide how many images to capture before a trigger is activated. Up to 7 images can be generated.

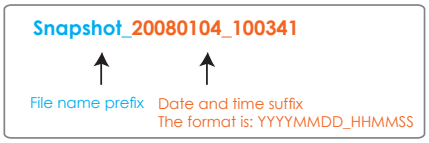
■ Send ☐ post-event images
Enter a number to decide how many images to capture after a trigger is activated. Up to 7 images can be generated.

For example, if both the Send pre-event images and Send post-event images are set to 7, a total of 15 images are generated after a trigger is activated.



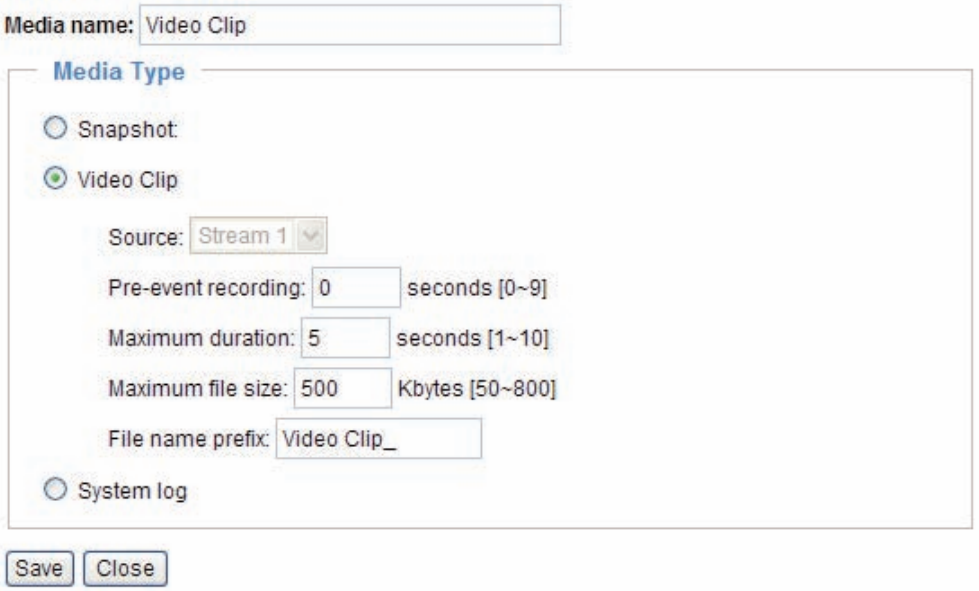
■ File name prefix
Enter the text that will be appended to the front of the file name.

■ Add date and time suffix to the file name
Select this option to add a date/time suffix to the file name.
For example:



Click **Save** to enable the settings, then click **Close** to exit the page.

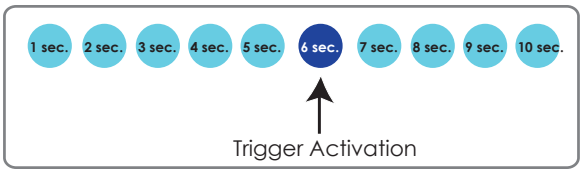
Video clip: Select to send video clips when a trigger is activated.



- Source: The source of video clip, which will be identical to the time shift caching stream. For more information about time shift caching stream, please refer to page 58.

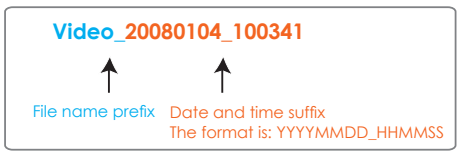
- Pre-event recording
  The Network Camera has a buffer area; it temporarily holds data up to a certain limit. Enter a number to decide the duration of recording before a trigger is activated. Up to 9 seconds can be set.

- Maximum duration
  Specify the maximum recording duration in seconds. Up to 10 seconds can be set.
  For example, if pre-event recording is set to five seconds and the maximum duration is set to ten seconds, the Network Camera continues to record for another 4 seconds after a trigger is activated.



- Maximum file size
  Specify the maximum file size allowed.

- File name prefix
  Enter the text that will be appended to the front of the file name.
  For example:

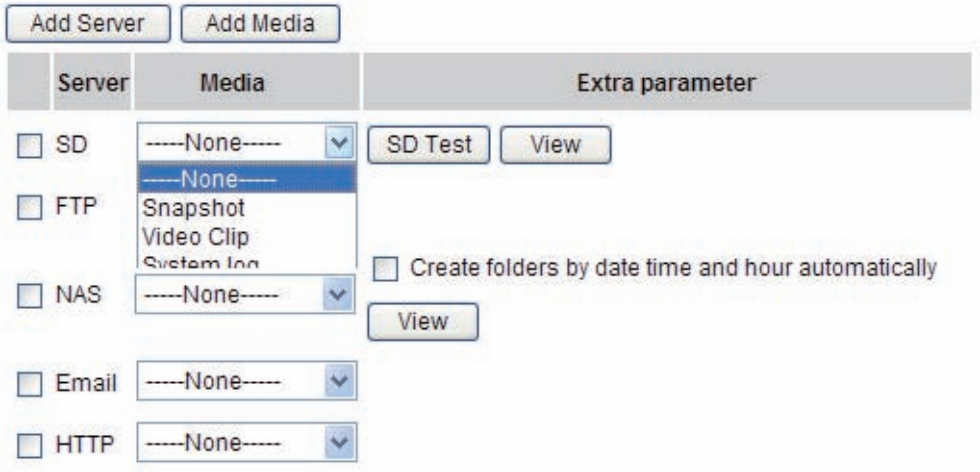


Click **Save** to enable the settings, then click **Close** to exit the page.

System log: Select to send a system log when a trigger is activated.
Click **Save** to enable the settings, then click **Close** to exit the page.

When completed, click **Save** to enable the settings and click **Close** to exit this page. The new media settings will appear on the Event Settings page.

You can continue to select a server and media type for the event. Please go back to page 66 for detailed information.



- SD Test: Click to test your SD card. The system will display a message indicating success or failure. If you want to use your SD card for local storage, please format it before use. Please refer to page 98 for detailed information.

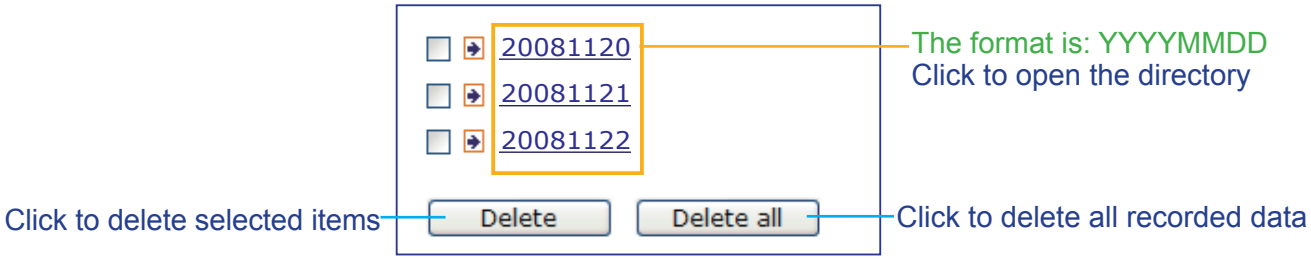
- Create folders by date, time, and hour automatically: If you check this item, the system will generate folders automatically by date.

- View: Click this button to open a file list window. This function is only for **SD card** and **Network Storage**.

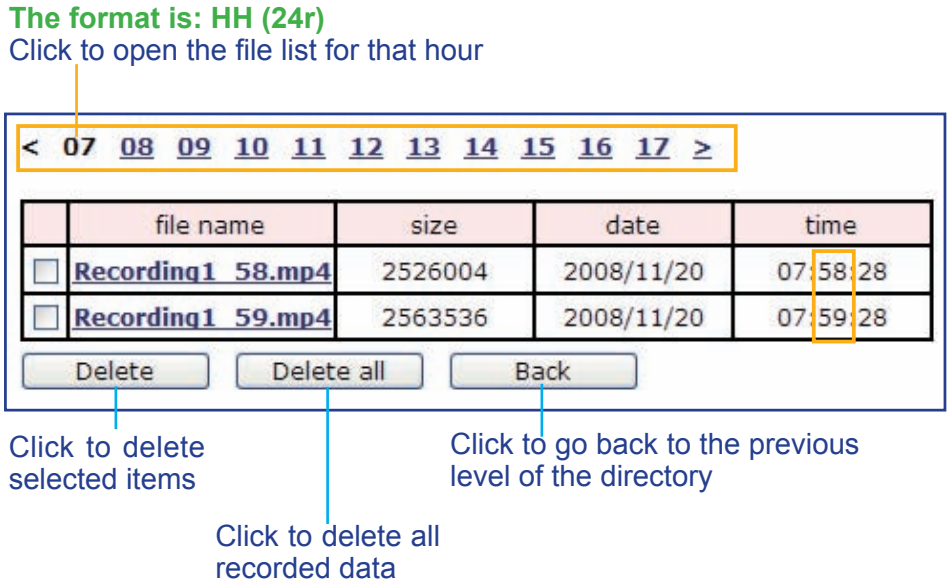
  If you click **View** button of SD card, a **Local storage** page will pop up for you to manage recorded files on SD card. For more information about Local storage, please refer to page 101 for illustration.

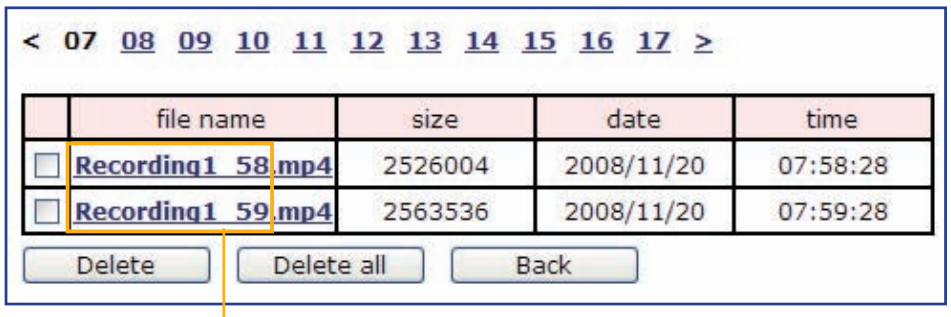
  If you click **View** button of Network storage, a **file directory window** will pop up for you to view recorded data on Network storage. For detailed illustration, please refer to the next page.

The following is an example of a file destination with video clips:



Click **20081120** to open the directory:

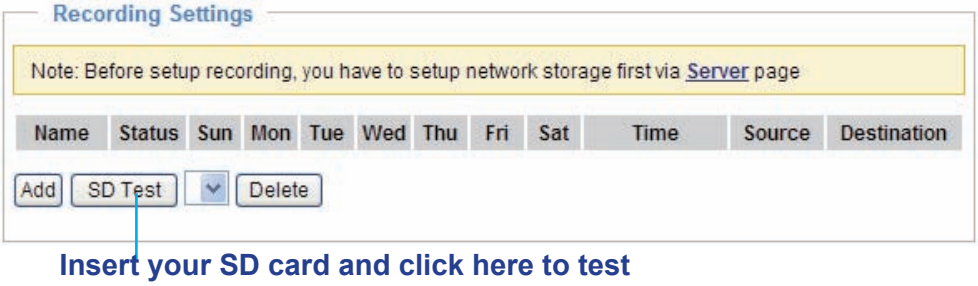




Recording Advanced Mode

This section explains how to configure the recording settings for the Network Camera.

Recording Settings



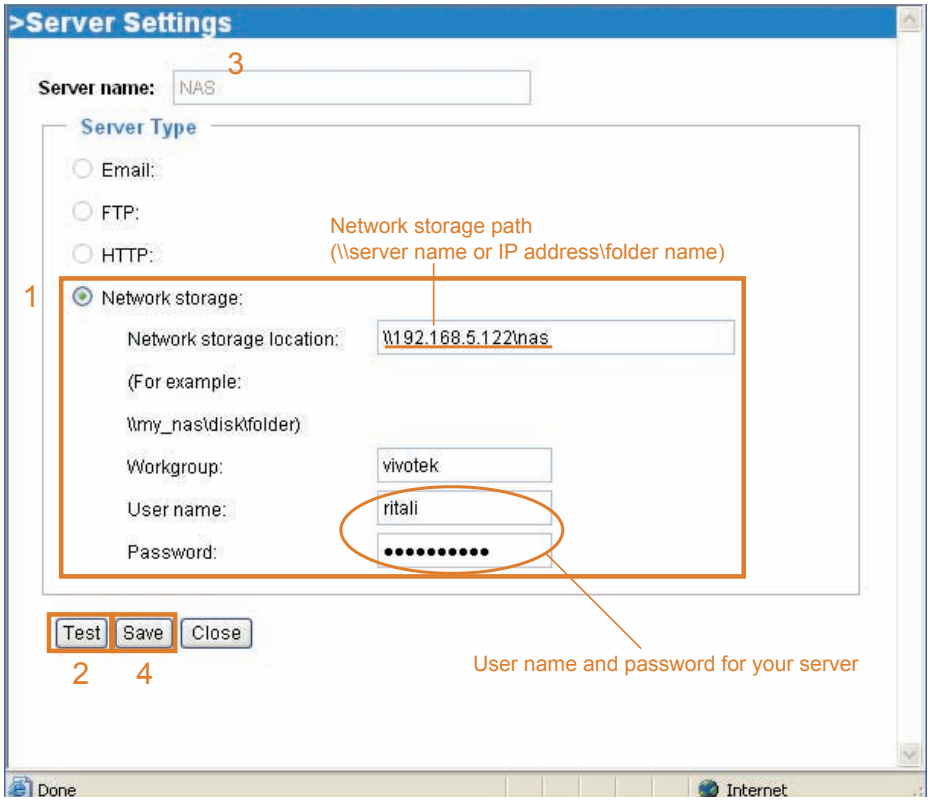
NOTE

► *Before setting up this page, please set up the Network Storage on the Server Settings page first.*
► *Please remember to format your SD card when using for the first time. Please refer to page 101 for detailed information.*

Network Storage Setting

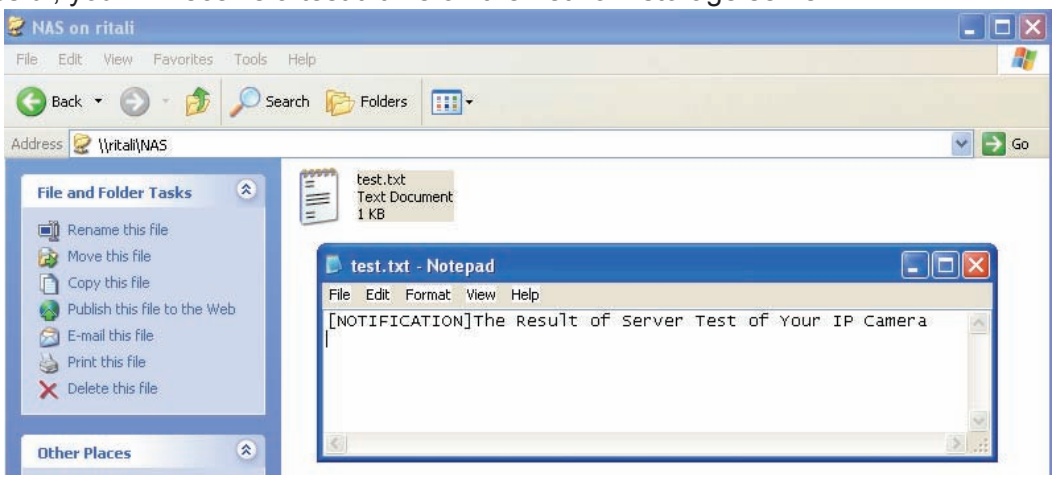
Click Server to open the Server Settings page and follow the steps below to set up:

1. Fill in the information for your server.
   For example:



2. Click **Test** to check the setting. The result will be shown in the pop-up window.

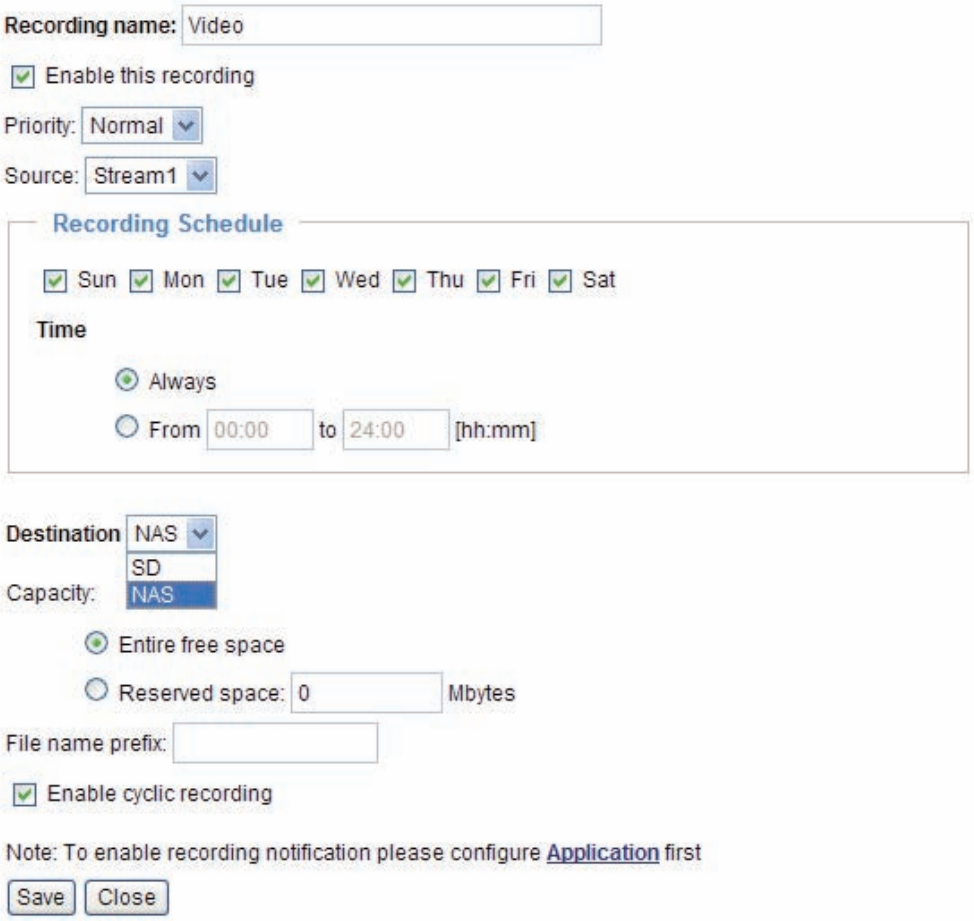
If successful, you will receive a test.txt file on the network storage server.



3. Enter a server name.
4. Click **Save** to complete the settings and click **Close** to exit the page.

Recording Settings

Click **Add** to open the recording setting page. In this page, you can define the recording source, recording schedule, and recording capacity. A total of 2 recording settings can be configured.



Recording name: Enter a name for the recording setting.

Enable this recording: Select this option to enable video recording.

Priority: Select the relative importance of this recording setting (High, Normal, and Low).

Source: Select the recording source (stream 1 ~ 4).

Recording Schedule: Specify the recording duration.

■ Select the days of the week.

■ Select the recording start and end times in 24-hr time format.

Destination: You can select the SD card or network storage that was set up for the recorded video files.

Capacity: You can choose either the entire free space available or limit the reserved space. The recording size limit must be larger than the reserved amount for cyclic recording.

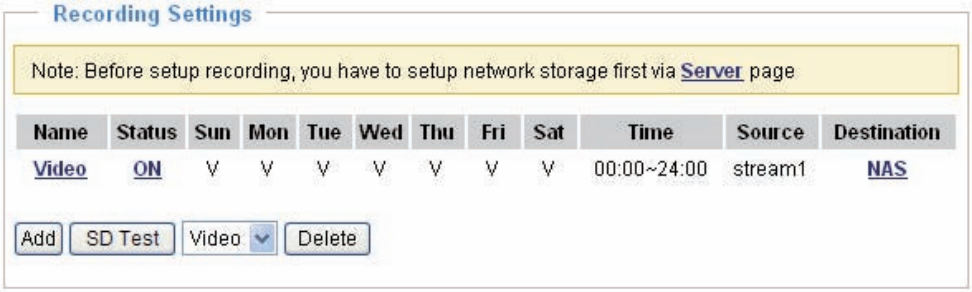
File name prefix: Enter the text that will be appended to the front of the file name.

Enable cyclic recording: If you check this item, when the maximum capacity is reached, the oldest file will be overwritten by the latest one.

If you want to enable recording notification, please click **Application** to set up. Please refer to **Trigger > Recording notify** on page 88 for detailed information.

When completed, select **Enable this recording**. Click **Save** to enable the setting and click **Close** to exit this page. When the system begins recording, it will send the recorded files to the Network Storage. The new recording name will appear in the drop-down list on the recording page as shown below.

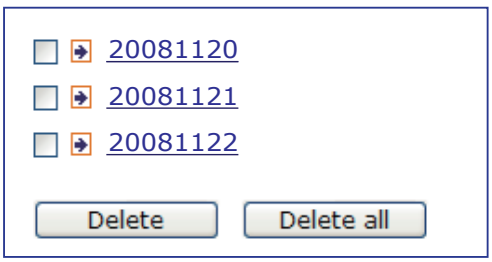
To remove a recording setting from the list, select a recording name from the drop-down list and click **Delete**.



■ Click **Video (Name)**: Opens the Recording Settings page to modify.

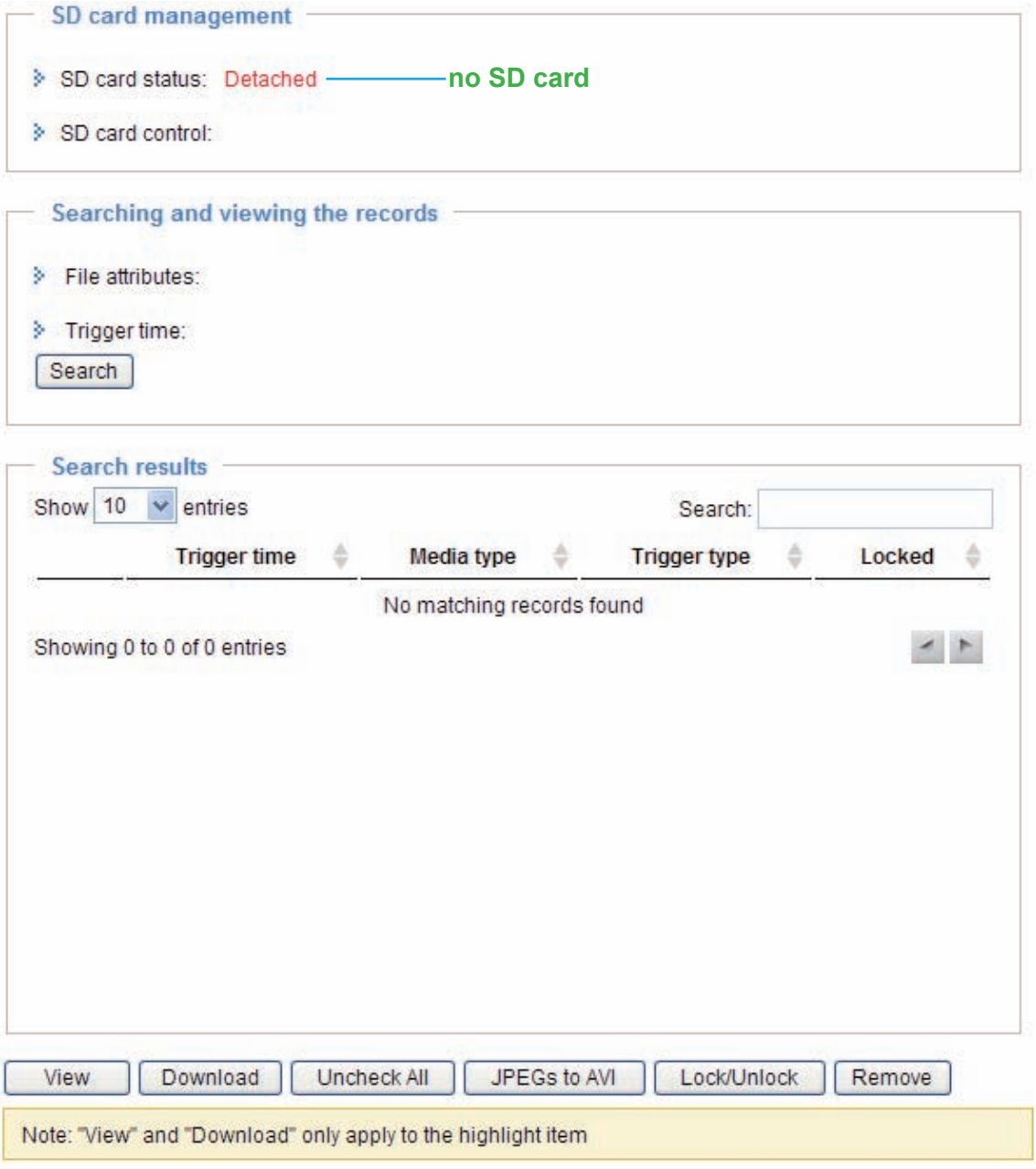
■ Click **ON (Status)**: The Status will become **OFF** and stop recording.

■ Click **NAS (Destination)**: Opens the file list of recordings as shown below. For more information about folder naming rules, please refer to page 97 for details.



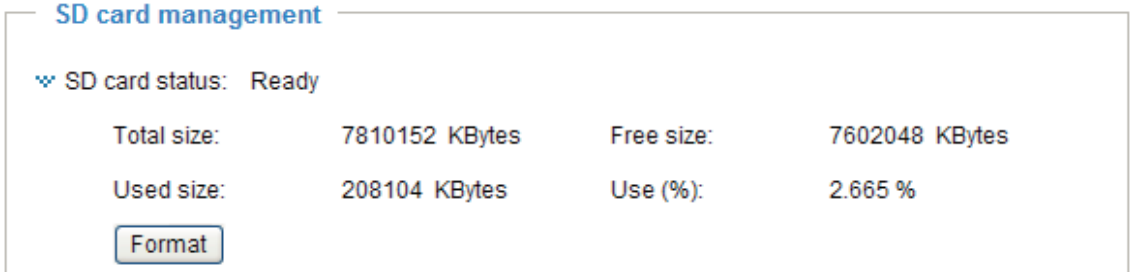
Local Storage Advanced Mode

This section explains how to manage the local storage on the Network Camera. Here you can view SD card status, search for recorded files to playback, download, etc.



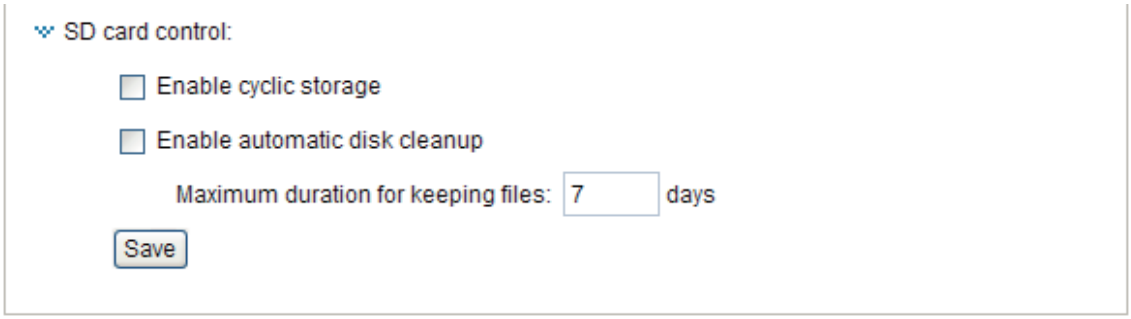
SD Card Management

SD card status: This column shows the status and reserved space of your SD card. Please remember to format the SD card when using for the first time.



SD card control

■ Enable cyclic storage: Check this item if you want to enable cyclic recording. When the maximum capacity is reached, the oldest file will be overwritten by the latest one.

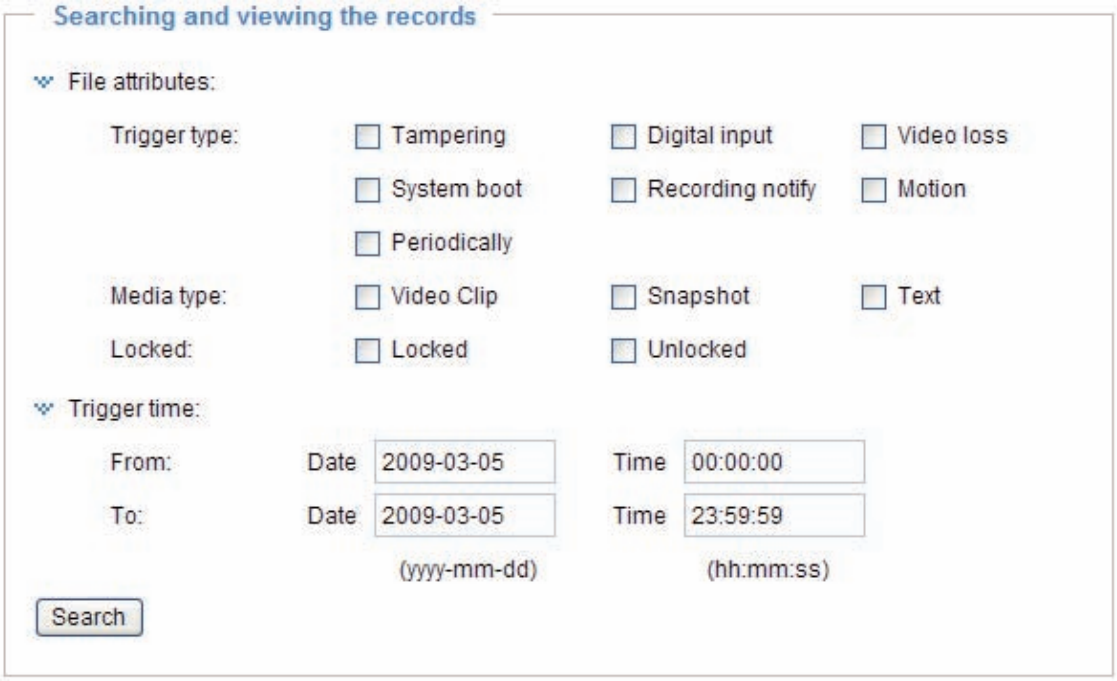


■ Enable automatic disk cleanup: Check this item and enter the number of days you wish to retain a file. For example, if you enter “7 days”, the recorded files will be stored on the SD card for 7 days.

Click **Save** to enable your settings.

Searching and Viewing the Records

This column allows the user to set up search criteria for recorded data. If you do not select any criteria and click **Search** button, all recorded data will be listed in the **Search Results** cloumn.



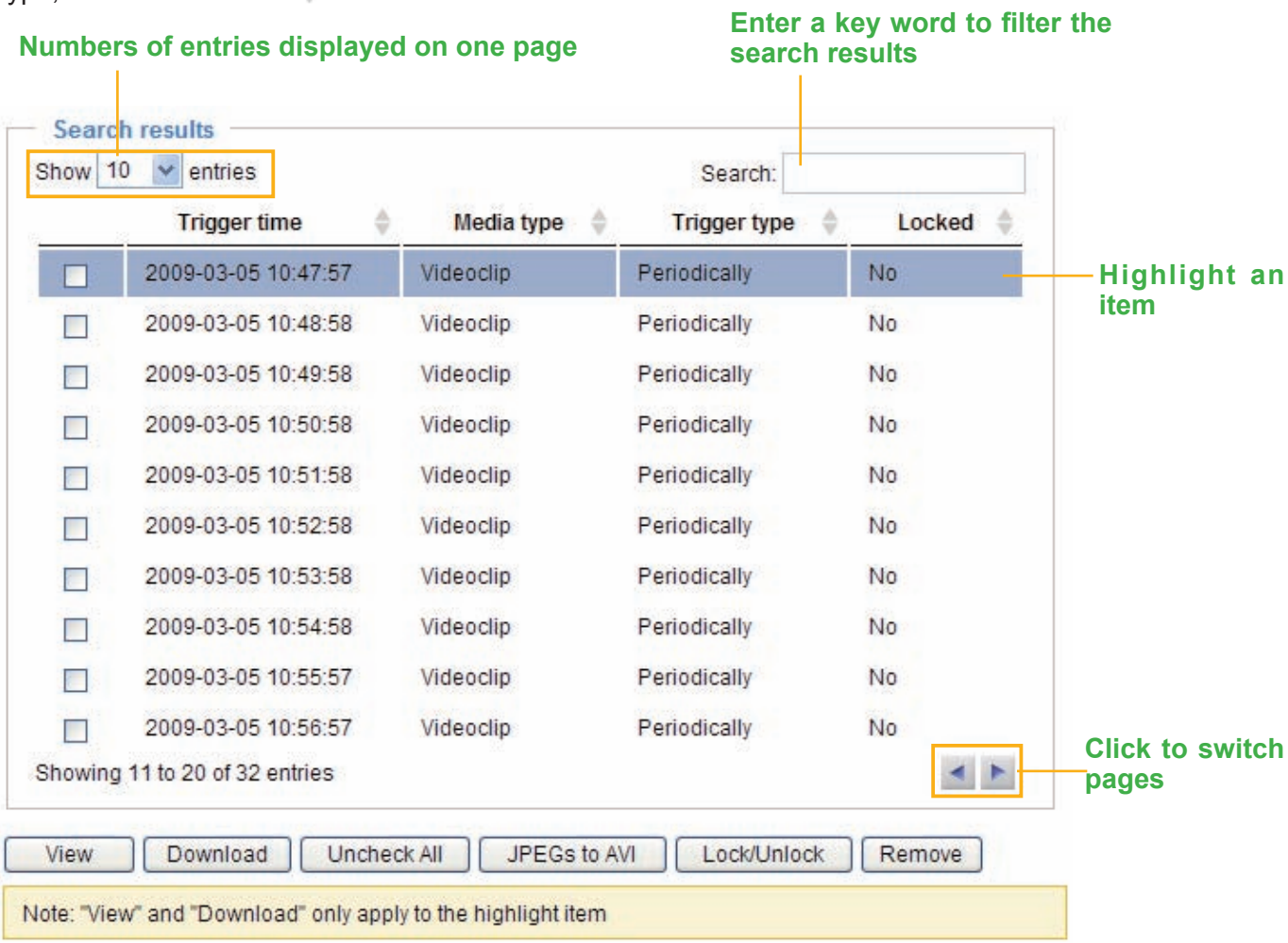
File attributes: Select one or more items as your search criteria.

Trigger time: Manually enter the time range you want to search.

Click **Search** and the recorded data corresponding to the search criteria will be listed in **Search Results** window.

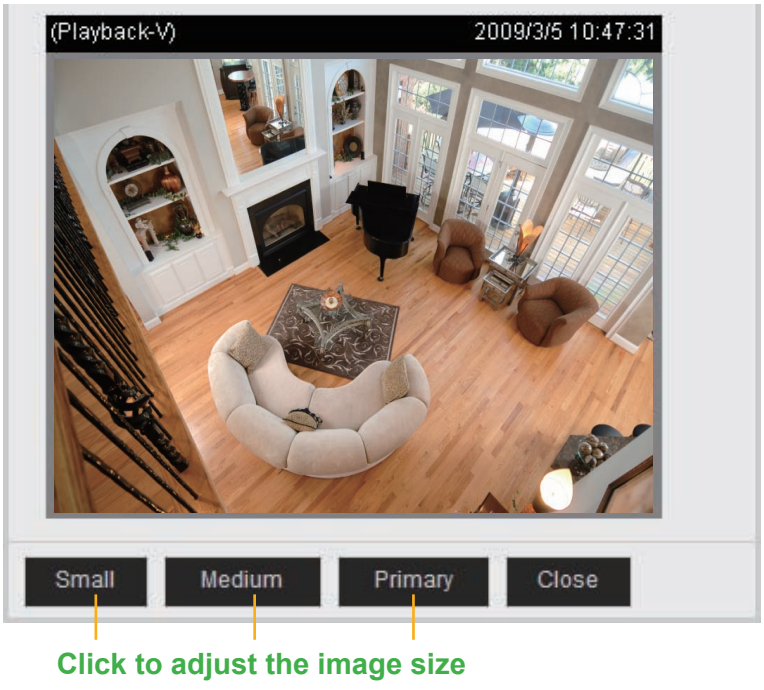
Search Results

The following is an example of search results. There are four columns: Trigger time, Media type, Trigger type, and Locked. Click ⇕ to sort the search results in either direction.



View: Click on a search result which will highlight the selected item in purple as shown above. Click the **View** button and a media window will pop up to play back the selected file.

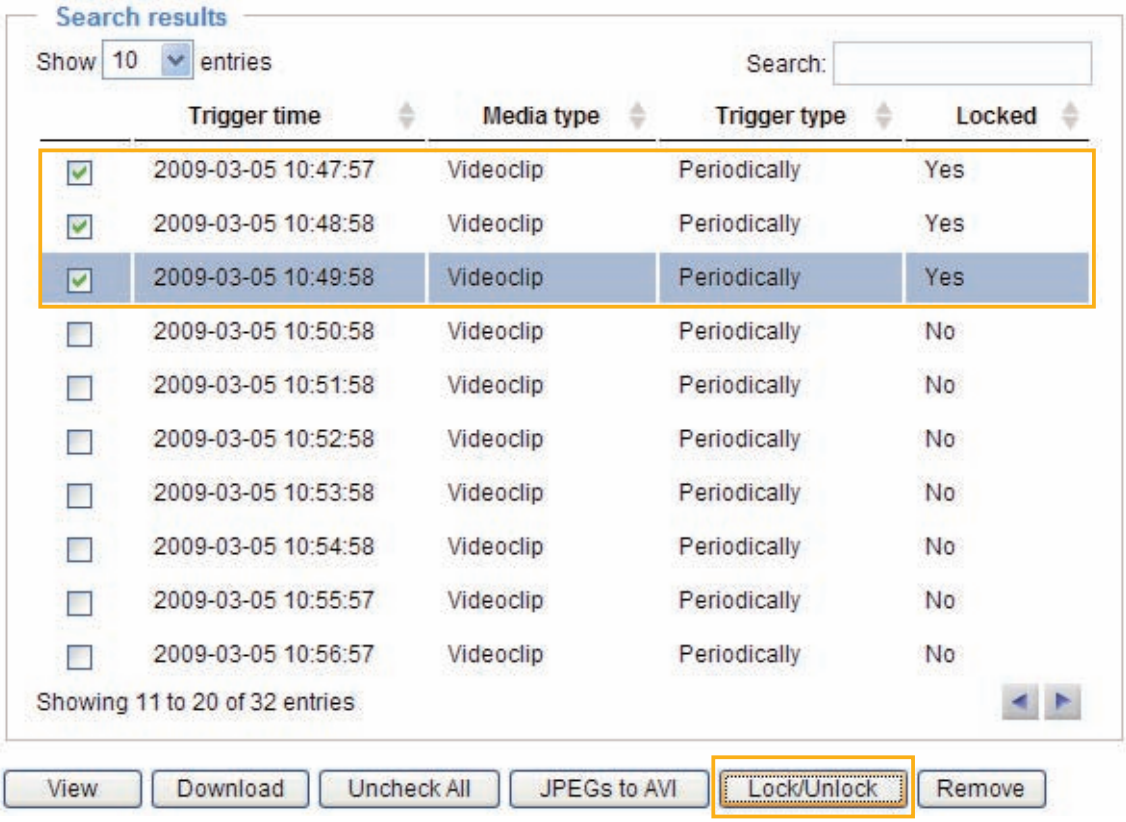
For example:



Download: Click on a search result to highlight the selected item in purple as shown above. Then click the **Download** button and a file download window will pop up for you to save the file.

JPEGs to AVI: This functions only applies to “JPEG“ format files such as snapshots. You can select several snapshots from the list, then click this button. Those snapshots will be converted into an AVI file.

Lock/Unlock: Select the desired search results, then click this button. The selected items will become Locked, which will not be deleted during cyclic recoroding. You can click again to unlock the selections. For example:

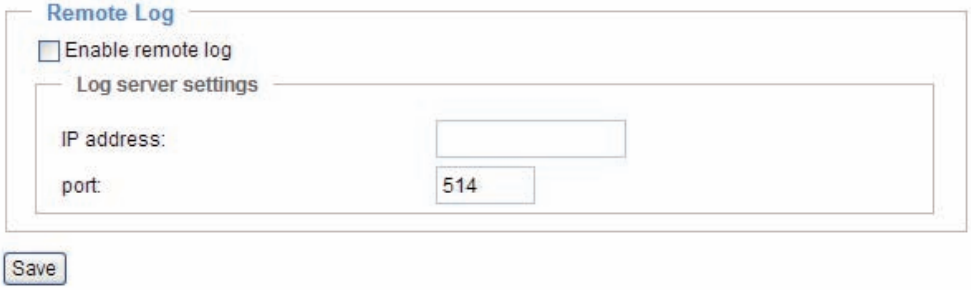


Remove: Select the desired search results, then click this button to delete the files.

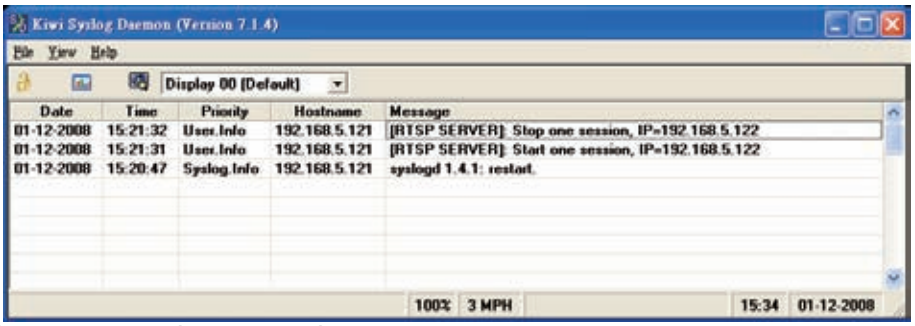
System Log Advanced Mode

This section explains how to configure the Network Camera to send the system log to the remote server as backup.

Remote Log

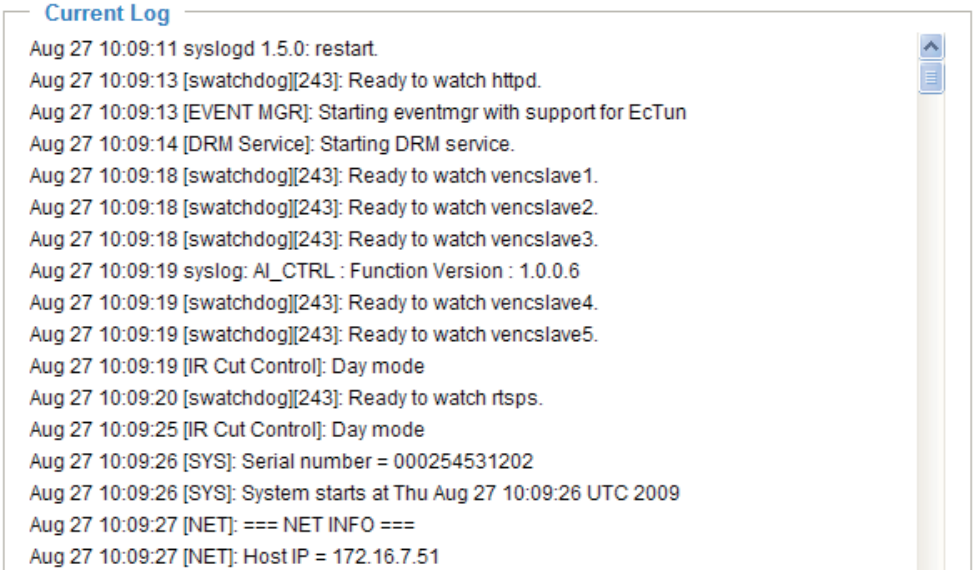


You can configure the Network Camera to send the system log file to a remote server as a log backup. Before utilizing this feature, it is suggested that the user install a log-recording tool to receive system log messages from the Network Camera. An example is Kiwi Syslog Daemon. Visit http://www.kiwisyslog.com/kiwi-syslog-daemon-overview/.



Follow the steps below to set up the remote log:
1. In the IP address text box, enter the IP address of the remote server.
2. In the port text box, enter the port number of the remote server.
3. When completed, select **Enable remote log** and click **Save** to enable the setting.

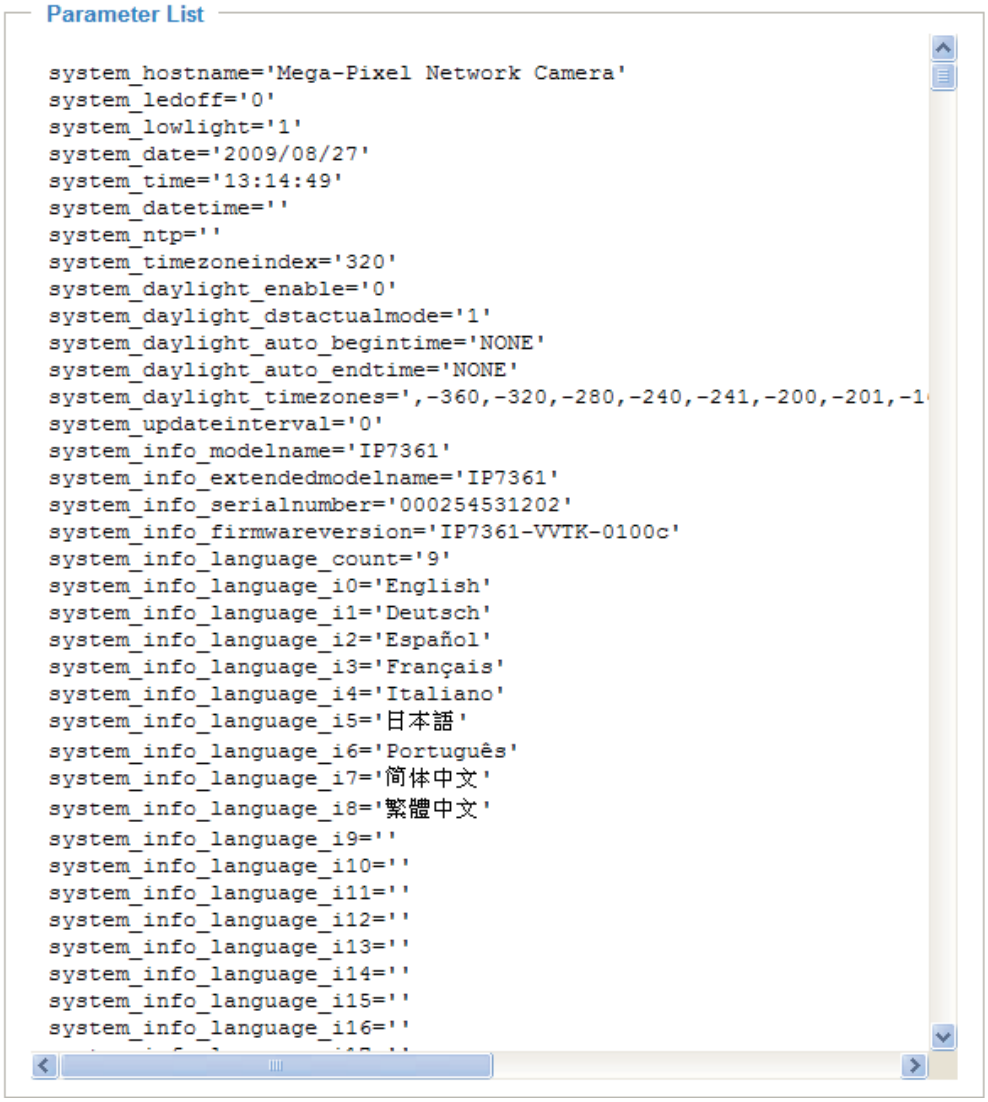
Current Log



This column displays the system log in chronological order. The system log is stored in the Network Camera's buffer area and will be overwritten when reaching a certain limit.

View Parameters Advanced Mode

The View Parameters page lists the entire system's parameters in alphabetical order. If you need technical assistance, please provide the information listed on this page.

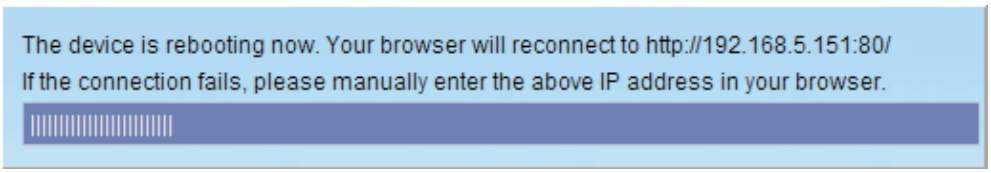


Maintenance

This chapter explains how to restore the Network Camera to factory default, upgrade firmware version, etc.

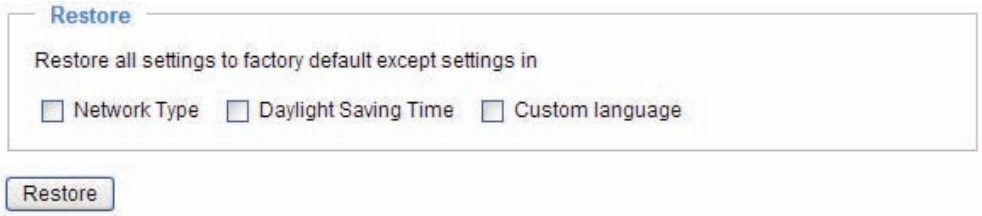
Reboot

This feature allows you to reboot the Network Camera, which takes about one minute to complete. When completed, the live video page will be displayed in your browser. The following message will be displayed during the reboot process.



If the connection fails after rebooting, manually enter the IP address of the Network Camera in the address field to resume the connection.

Restore



This feature allows you to restore the Network Camera to factory default settings.

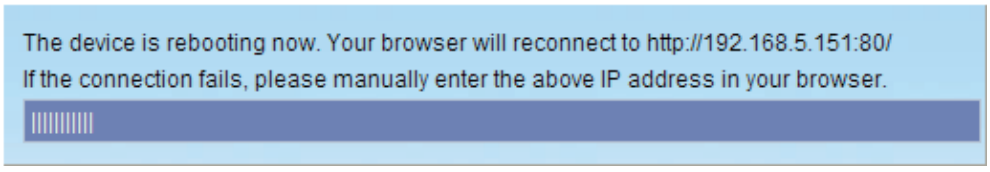
Network Type: Select this option to retain the Network Type settings (please refer to Network Type on page 38).

Daylight Saving Time: Select this option to retain the Daylight Saving Time settings (please refer to System on page 29).

Custom Language: Select this option to retain the Custom Language settings.

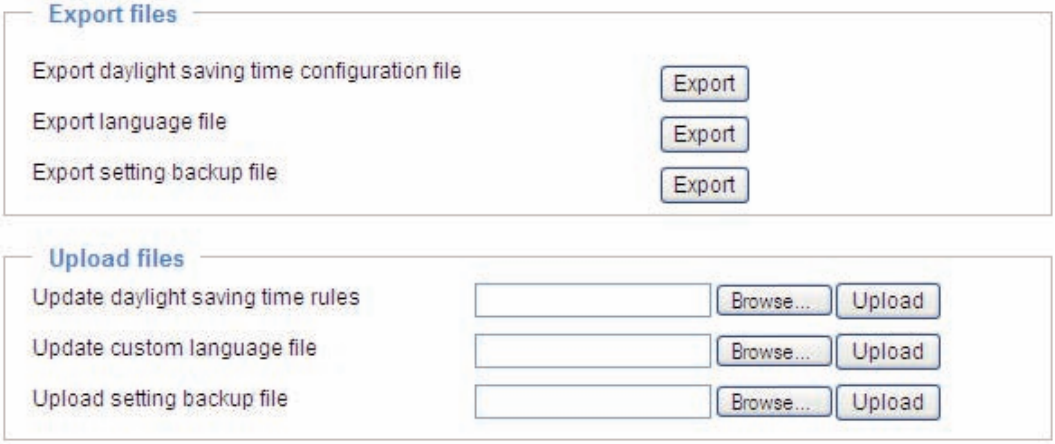
If none of the options is selected, all settings will be restored to factory default.

The following message is displayed during the restoring process.



Export / Upload Files Advanced Mode

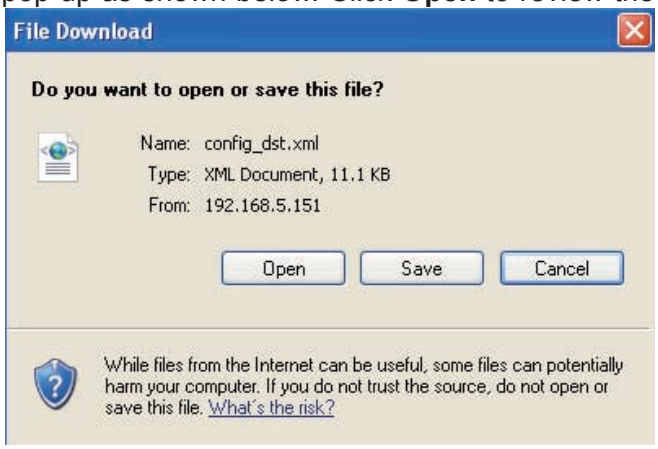
This feature allows you to Export / Upload daylight saving time rules, custom language files, and setting backup files.



Export daylight saving time configuration file: Click to set the start and end time of DST.

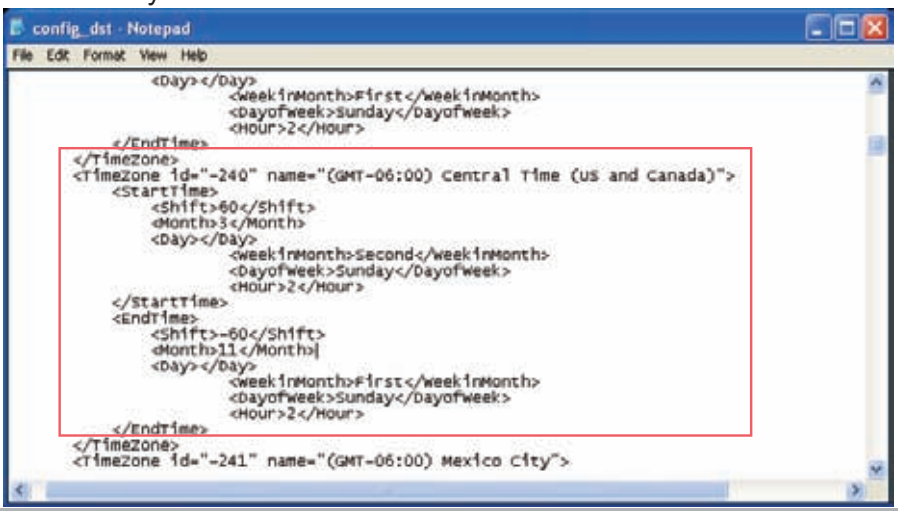
Follow the steps below to export:

1. In the Export files column, click **Export** to export the daylight saving time configuration file from the Network Camera.
2. A file download dialog will pop up as shown below. Click **Open** to review the XML file or click **Save** to store the file for editing.



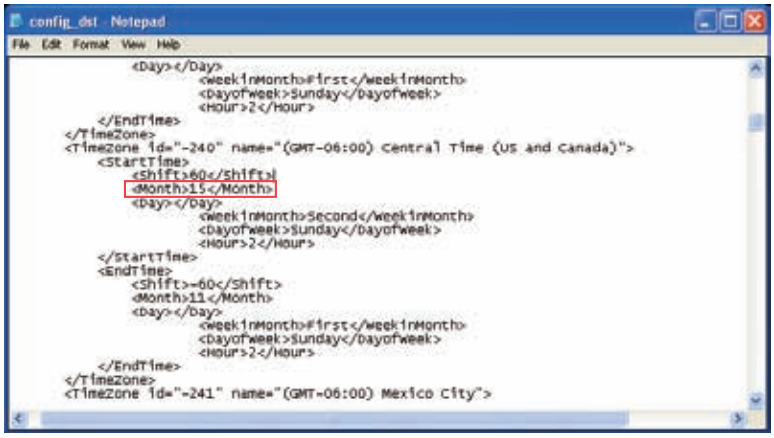
3. Open the file with Microsoft® Notepad and locate your time zone; set the start and end time of DST. When completed, save the file.

In the example below, DST begins each year at 2:00 a.m. on the second Sunday in March and ends at 2:00 a.m. on the first Sunday in November.



Upload daylight saving time rule: Click **Browse…** and specify the XML file to upload.

If the incorrect date and time are assigned, you will see the following warning message when uploading the file to the Network Camera.



The following message is displayed when attempting to upload an incorrect file format.

Export language file: Click to export language strings. VIVOTEK provides nine languages: English, Deutsch, Español, Français, Italiano, 日本語, Português, 簡体中文, and 繁體中文.

Upload custom language file: Click **Browse…** and specify your own custom language file to upload.

Export setting backup file: Click to export all parameters for the device and user-defined scripts.

Upload setting backup file: Click **Browse…** to upload a setting backup file. Please note that the model and firmware version of the device should be the same as the setting backup file. If you have set up a fixed IP or other special settings for your device, it is not suggested to upload a settings backup file.

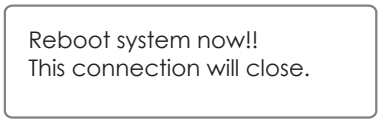
Upgrade Firmware

This feature allows you to upgrade the firmware of your Network Camera. It takes a few minutes to complete the process.
Note: Do not power off the Network Camera during the upgrade!

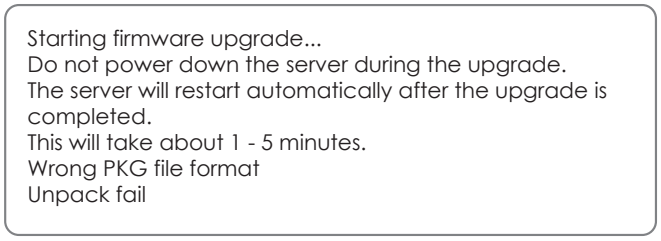
Follow the steps below to upgrade the firmware:
1. Download the latest firmware file from the VIVOTEK website. The file is in .pkg file format.
2. Click **Browse…** and specify the firmware file.
3. Click **Upgrade**. The Network Camera starts to upgrade and will reboot automatically when the upgrade completes.

If the upgrade is successful, you will see “Reboot system now!! This connection will close”. After that, re-access the Network Camera.

The following message is displayed when the upgrade has succeeded.



The following message is displayed when you have selected an incorrect firmware file.



Appendix

URL Commands for the Network Camera

Overview

For some customers who already have their own web site or web control application, the Network Camera/Video Server can be easily integrated through URL syntax. This section specifies the external HTTP-based application programming interface. The HTTP-based camera interface provides the functionality to request a single image, control camera functions (PTZ, output relay etc.), and get and set internal parameter values. The image and CGI-requests are handled by the built-in Web server.

Style Convention

In URL syntax and in descriptions of CGI parameters, text within angle brackets denotes content that is to be replaced with either a value or a string. When replacing the text string, the angle brackets should also be replaced. An example of this is the description of the name for the server, denoted with <servername> in the URL syntax description below, that is replaced with the string myserver in the URL syntax example further down in the page.

URL syntax is denoted with the word "Syntax:" written in bold face followed by a box with the referenced syntax as shown below. For example, name of the server is written as <servername> and is intended to be replaced with the name of the actual server. This can either be a name, e.g., "mywebcam" or "thecam.adomain.net" or the associated IP number for the server, e.g., 192.168.0.220.

Syntax:

```
http://<servername>/cgi-bin/viewer/video.jpg
```

Description of returned data is written with "**Return:**" in bold face followed by the returned data in a box. All data is returned in HTTP format, i.e., each line is separated with a Carriage Return and Line Feed (CRLF) printed as \r\n.

Return:

```
HTTP/1.0 <HTTP code> <HTTP text>\r\n
```

URL syntax examples are written with "**Example:**" in bold face followed by a short description and a light grey box with the example.

Example: request a single snapshot image

```
http://mywebserver/cgi-bin/viewer/video.jpg
```

1. General CGI URL Syntax and Parameters

CGI parameters are written in lower-case and as one word without any underscores or other separators. When the CGI request includes internal camera parameters, these parameters must be written exactly as they are named in the camera or video server. The CGIs are organized in functionally-related directories under the cgi-bin directory. The file extension .cgi is required.

Syntax:

http://<*servername*>/cgi-bin/<*subdir*>[/<*subdir*>...]/<*cgi*>.<*ext*>
[?<parameter>=<value>[&<parameter>=<value>...]]

Example: Set digital output #1 to active

http://mywebserver/cgi-bin/dido/setdo.cgi?do1=1

2. Security Level

SECURITY LEVEL	SUB-DIRECTORY	DESCRIPTION
0	anonymous	Unprotected.
1 [view]	anonymous, viewer, dido, camctrl	1. Can view, listen, talk to camera. 2. Can control DI/DO, PTZ of the camera.
4 [operator]	anonymous, viewer, dido, camctrl, operator	Operator access rights can modify most of the camera's parameters except some privileges and network options.
6 [admin]	anonymous, viewer, dido, camctrl, operator, admin	Administrator access rights can fully control the camera's operations.
7	N/A	Internal parameters. Unable to be changed by any external interfaces.

3. Get Server Parameter Values

Note: The access right depends on the URL directory.

Method: GET/POST

Syntax:

http://<*servername*>/cgi-bin/anonymous/getparam.cgi?[<*parameter*>]
[&<parameter>…]

http://<*servername*>/cgi-bin/viewer/getparam.cgi?[<*parameter*>]
[&<parameter>…]

http://<*servername*>/cgi-bin/operator/getparam.cgi?[<*parameter*>]
[&<parameter>…]

http://<*servername*>/cgi-bin/admin/getparam.cgi?[<*parameter*>]
[&<parameter>…]

Where the <*parameter*> should be <*group*>[_<*name*>] or <*group*>[.<*name*>]. If you do not specify any parameters, all the parameters on the server will be returned. If you specify only <*group*>, the parameters of the related group will be returned.

When querying parameter values, the current parameter values are returned.

A successful control request returns parameter pairs as follows:

Return:

HTTP/1.0 200 OK\r\n
Content-Type: text/html\r\n
Context-Length: <length>\r\n
\r\n
<*parameter pair*>

where <parameter pair> is

<parameter>=<value>\r\n
[<parameter pair>]

<length> is the actual length of content.

Example: Request IP address and its response

Request:

http://192.168.0.123/cgi-bin/admin/getparam.cgi?network_ipaddress

Response:

HTTP/1.0 200 OK\r\n

Content-Type: text/html\r\n

Context-Length: 33\r\n

\r\n

network.ipaddress=192.168.0.123\r\n

4. Set Server Parameter Values

Note: The access right depends on the URL directory.

Method: GET/POST

Syntax:

http://<*servername*>/cgi-bin/anonymous/setparam.cgi? <*parameter*>=<*value*>
[&<parameter>=<value>…][&update=<value>][&return=<return page>]

http://<*servername*>/cgi-bin/viewer/setparam.cgi? <*parameter*>=<*value*>
[&<parameter>=<value>…][&update=<value>] [&return=<return page>]

http://<*servername*>/cgi-bin/operator/setparam.cgi? <*parameter*>=<*value*>
[&<parameter>=<value>…][&update=<value>] [&return=<return page>]

http://<*servername*>/cgi-bin/admin/setparam.cgi? <*parameter*>=<*value*>
[&<parameter>=<value>…][&update=<value>] [&return=<return page>]

PARAMETER	VALUE	DESCRIPTION
<group>_<name>	value to assigned	Assign <*value*> to the parameter <*group*>_<*name*>.
update	<boolean>	Set to 1 to update all fields (no need to update parameter in each group).
return	<*return page*>	Redirect to the page <*return page*> after the parameter is assigned. The <*return page*> can be a full URL path or relative path according to the current path. If you omit this parameter, it will redirect to an empty page. (Note: The return page can be a general HTML file (.htm, .html) or a VIVOTEK server script executable (.vspx) file. It cannot be a CGI command or have any extra parameters. This parameter must be placed at the end of the parameter list.

Return:

HTTP/1.0 200 OK\r\n
Content-Type: text/html\r\n
Context-Length: <length>\r\n
\r\n
<*parameter pair*>

where <parameter pair> is

<parameter>=<value>\r\n
[<parameter pair>]

Only the parameters that you set and are readable will be returned.

Example: Set the IP address of server to 192.168.0.123:

Request:

http://myserver/cgi-bin/admin/setparam.cgi?network_ipaddress=192.168.0.123

Response:

HTTP/1.0 200 OK\r\n

Content-Type: text/html\r\n

Context-Length: 33\r\n

\r\n

network.ipaddress=192.168.0.123\r\n

5. Available Parameters on the Server

This chapter defines all the parameters which can be configured or retrieved from VIVOTEK network camera or video server. The general format of description is listed in the table below

Valid values:

VALID VALUES	DESCRIPTION
string[<n>]	Text strings shorter than 'n' characters. The characters ",', <,>,& are invalid.
string[n~m]	Text strings longer than `n' characters and shorter than `m' characters. The characters ",', <,>,& are invalid.
password[<n>]	The same as string but displays '*' instead.
integer	Any number between $(-2^{31} - 1)$ and $(2^{31} - 1)$.
positive integer	Any number between 0 and $(2^{32} - 1)$.
<m> ~ <n>	Any number between 'm' and 'n'.
domain name[<n>]	A string limited to a domain name shorter than 'n' characters (eg. www.ibm.com).
email address [<n>]	A string limited to an email address shorter than 'n' characters (eg. joe@www.ibm.com).
ip address	A string limited to an IP address (eg. 192.168.1.1).
mac address	A string limited to contain a MAC address without hyphens or colons.
boolean	A boolean value of 1 or 0 represents [Yes or No], [True or False], [Enable or Disable].
<value1>, <value2>, <value3>, …	Enumeration. Only given values are valid.
blank	A blank string.
everything inside <>	A description
integer primary key	SQLite data type. A 32-bit signed integer. The value is assigned a unique integer by the server.
text	SQLite data type. The value is a text string, stored using the database encoding (UTF-8, UTF-16BE or UTF-16-LE).
coordinate	x, y coordinate (eg. 0,0)
window size	window width and height (eg. 800x600)

NOTE: The camera should not be restarted when parameters are changed.

5.1 System

Group: **system**

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
hostname	string[40]	1/6	Host name of server (Network Camera, Wireless Network Camera, Video Server, Wireless Video Server).
ledoff	<boolean>	6/6	Turn on (0) or turn off (1) all led indicators.
lowlight	<boolean>	6/6	Turn on white light LED under all conditions. Only turn on white light LED in low light conditions. (product dependent)
date	<yyyy/mm/dd>, keep, auto	6/6	Current date of system. Set to 'keep' to keep date unchanged. Set to 'auto' to use NTP to synchronize date.
time	<hh:mm:ss>, keep, auto	6/6	Current time of the system. Set to 'keep' to keep time unchanged. Set to 'auto' to use NTP to synchronize time.
datetime	<MMDDhhmm YYYY.ss>	6/6	Another current time format of the system.
ntp	<domain name>, <ip address>, <blank>	6/6	NTP server. *Do not use "skip to invoke default server" for default value.
timezoneindex	-489 ~ 529	6/6	Indicate timezone and area. -480: GMT-12:00 Eniwetok, Kwajalein -440: GMT-11:00 Midway Island, Samoa -400: GMT-10:00 Hawaii -360: GMT-09:00 Alaska -320: GMT-08:00 Las Vegas, San_Francisco, Vancouver -280: GMT-07:00 Mountain Time, Denver -281: GMT-07:00 Arizona -240: GMT-06:00 Central America, Central Time, Mexico City, Saskatchewan -200: GMT-05:00 Eastern Time, New York, Toronto -201: GMT-05:00 Bogota, Lima, Quito, Indiana -180: GMT-04:30 Caracas -160: GMT-04:00 Atlantic Time, Canada, La Paz, Santiago -140: GMT-03:30 Newfoundland -120: GMT-03:00 Brasilia, Buenos Aires, Georgetown, Greenland -80: GMT-02:00 Mid-Atlantic -40: GMT-01:00 Azores, Cape_Verde_IS.

			0: GMT Casablanca, Greenwich Mean Time: Dublin, Edinburgh, Lisbon, London 40: GMT 01:00 Amsterdam, Berlin, Rome, Stockholm, Vienna, Madrid, Paris 41: GMT 01:00 Warsaw, Budapest, Bern 80: GMT 02:00 Athens, Helsinki, Istanbul, Riga 81: GMT 02:00 Cairo 82: GMT 02:00 Lebanon, Minsk 83: GMT 02:00 Israel 120: GMT 03:00 Baghdad, Kuwait, Riyadh, Moscow, St. Petersburg, Nairobi 121: GMT 03:00 Iraq 140: GMT 03:30 Tehran 160: GMT 04:00 Abu Dhabi, Muscat, Baku, Tbilisi, Yerevan 180: GMT 04:30 Kabul 200: GMT 05:00 Ekaterinburg, Islamabad, Karachi, Tashkent 220: GMT 05:30 Calcutta, Chennai, Mumbai, New Delhi 230: GMT 05:45 Kathmandu 240: GMT 06:00 Almaty, Novosibirsk, Astana, Dhaka, Sri Jayawardenepura 260: GMT 06:30 Rangoon 280: GMT 07:00 Bangkok, Hanoi, Jakarta, Krasnoyarsk 320: GMT 08:00 Beijing, Chongging, Hong Kong, Kuala Lumpur, Singapore, Taipei 360: GMT 09:00 Osaka, Sapporo, Tokyo, Seoul, Yakutsk 380: GMT 09:30 Adelaide, Darwin 400: GMT 10:00 Brisbane, Canberra, Melbourne, Sydney, Guam, Vladivostok 440: GMT 11:00 Magadan, Solomon Is., New Caledonia 480: GMT 12:00 Aucklan, Wellington, Fiji, Kamchatka, Marshall Is. 520: GMT 13:00 Nuku'Alofa
daylight_enable	<boolean>	6/6	Enable automatic daylight saving time in time zone.
daylight_dstactualmode	<boolean>	6/7	Check if current time is under daylight saving time. (Used internally)
daylight_auto_begintime	string[19]	6/7	Display the current daylight saving start time. (product dependent)

daylight_auto_endtime	string[19]	6/7	Display the current daylight saving end time. (product dependent)
daylight_timezones	string	6/6	List time zone index which support daylight saving time.
updateinterval	0, 3600, 86400, 604800, 2592000	6/6	0 to Disable automatic time adjustment, otherwise, it indicates the seconds between NTP automatic update intervals.
restore	0, <positive integer>	7/6	Restore the system parameters to default values after <value> seconds.
reset	0, <positive integer>	7/6	Restart the server after <value> seconds if <value> is non-negative.
restoreexceptnet	<Any value>	7/6	Restore the system parameters to default values except (ipaddress, subnet, router, dns1, dns2, pppoe). This command can cooperate with other "restoreexceptXYZ" commands. When cooperating with others, the system parameters will be restored to the default value except for a union of the combined results.
restoreexceptdst	<Any value>	7/6	Restore the system parameters to default values except all daylight saving time settings. This command can cooperate with other "restoreexceptXYZ" commands. When cooperating with others, the system parameters will be restored to default values except for a union of combined results.
restoreexceptlang	<Any Value>	7/6	Restore the system parameters to default values except the custom language file the user has uploaded. This command can cooperate with other "restoreexceptXYZ" commands. When cooperating with others, the system parameters will be restored to the default value except for a union of the combined results.

5.1.1 System.info

Subgroup of **system**: **info** (The fields in this group are unchangeable.)

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
modelname	string[40]	0/7	Internal model name of the server (eg. IP7139)
extendedmodelname	string[40]	0/7	ODM specific model name of server (eg. DCS-5610). If it is not an ODM model, this field will be equal to "modelname"

serialnumber	<mac address>	0/7	12 characters MAC address (without hyphens).
firmwareversion	string[40]	0/7	Firmware version, including model, company, and version number in the format: <MODEL-BRAND-VERSION>
language_count	<integer>	0/7	Number of webpage languages available on the server.
language_i<0~(count-1)>	string[16]	0/7	Available language lists.
customlanguage_maxcount	<integer>	0/6	Maximum number of custom languages supported on the server.
customlanguage_count	<integer>	0/6	Number of custom languages which have been uploaded to the server.
customlanguage_i<0~(maxcount-1)>	string	0/6	Custom language name.

5.2 Status

Group: **status**

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
di_i<0~(ndi-1)>	<boolean>	1/7	0 => Inactive, normal 1 => Active, triggered
do_i<0~(ndo-1)>	<boolean>	1/7	0 => Inactive, normal 1 => Active, triggered
onlinenum_rtsp	integer	6/7	Current number of RTSP connections.
onlinenum_httppush	integer	6/7	Current number of HTTP push server connections.
eth_i0	<string>	1/99	Get network information from mii-tool.

5.3 Digital Input Behavior Define

Group: **di_i<0~(ndi-1)>** (capability.ndi > 0)

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
normalstate	high, low	1/1	Indicates open circuit or closed circuit (inactive status)

5.4 Digital Output Behavior Define

Group: **do_i<0~(ndo-1)>** (capability.ndo > 0)

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
normalstate	open, grounded	1/1	Indicate open circuit or closed circuit (inactive status)

5.5 Security

Group: security

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
privilege_do	view, operator, admin	6/6	Indicate which privileges and above can control digital output
privilege_camctrl	view, operator, admin	6/6	Indicate which privileges and above can control PTZ
user_i0_name	string[64]	6/7	User name of root
user_i<1~20>_name	string[64]	6/7	User name
user_i0_pass	password[64]	6/6	Root password
user_i<1~20>_pass	password[64]	7/6	User password
user_i0_privilege	viewer, operator, admin	6/7	Root privilege
user_i<1~20>_ privilege	viewer, operator, admin	6/6	User privilege

5.6 Network

Group: **network**

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
type	lan, pppoe	6/6	Network connection type.
preprocess	0~15	6/6	Stop related process before setting port value.
resetip	<boolean>	6/6	1 => Get ipaddress, subnet, router, dns1, dns2 from DHCP server at next reboot. 0 => Use preset ipaddress, subnet, rounter, dns1, and dns2.
ipaddress	<ip address>	6/6	IP address of server.
subnet	<ip address>	6/6	Subnet mask.
router	<ip address>	6/6	Default gateway.
dns1	<ip address>	6/6	Primary DNS server.
dns2	<ip address>	6/6	Secondary DNS server.
wins1	<ip address>	6/6	Primary WINS server.
wins2	<ip address>	6/6	Secondary WINS server.

5.6.1 802.1x

Subgroup of network: ieee8021x

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
enable	<boolean>	6/6	Enable/disable IEEE 802.1x
eapmethod	eap-peap, eap-tls	6/6	Selected EAP method
identity_peap	String[64]	6/6	PEAP identity
identity_tls	String[64]	6/6	TLS identity
password	String[254]	6/6	Password for TLS
privatekeypassword	String[254]	6/6	Password for PEAP
ca_exist	<boolean>	6/6	CA installed flag
ca_time	<integer>	6/7	CA installed time. Represented in EPOCH
ca_size	<integer>	6/7	CA file size (in bytes)
certificate_exist	<boolean>	6/6	Certificate installed flag (for TLS)
certificate_time	<integer>	6/7	Certificate installed time. Represented in EPOCH
certificate_size	<integer>	6/7	Certificate file size (in bytes)
privatekey_exist	<boolean>	6/6	Private key installed flag (for TLS)
privatekey_time	<integer>	6/7	Private key installed time. Represented in EPOCH
privatekey_size	<integer>	6/7	Private key file size (in bytes)

5.6.2 QOS

Subgroup of **network: qos**

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
cos_enable	<boolean>	6/6	Enable/disable CoS (IEEE 802.1p)
cos_vlanid	1~4095	6/6	VLAN ID
cos_video	0~7	6/6	Video channel for CoS
cos_audio	0~7	6/6	Audio channel for CoS
cos_eventalarm	0~7	6/6	Event/alarm channel for CoS
cos_management	0~7	6/6	Management channel for CoS
cos_eventtunnel	0~7	6/6	Event/Control channel for CoS
dscp_enable	<boolean>	6/6	Enable/disable DSCP
dscp_video	0~63	6/6	Video channel for DSCP
dscp_audio	0~63	6/6	Audio channel for DSCP
dscp_eventalarm	0~63	6/6	Event/alarm channel for DSCP
dscp_management	0~63	6/6	Management channel for DSCP
dscp_eventtunnel	0~63	6/6	Event/Control channel for DSCP

5.6.3 IPV6

Subgroup of **network**: **ipv6**

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
enable	<boolean>	6/6	Enable IPv6.
addonipaddress	<ip address>	6/6	IPv6 IP address.
addonprefixlen	0~128	6/6	IPv6 prefix length.
addonrouter	<ip address>	6/6	IPv6 router address.
addondns	<ip address>	6/6	IPv6 DNS address.
allowoptional	<boolean>	6/6	Allow manually setup of IP address setting.

5.6.4 FTP

Subgroup of **network**: **ftp**

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
Port	21, 1025~65535	6/6	Local ftp server port.

5.6.5 HTTP

Subgroup of **network**: **http**

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
port	80, 1025 ~ 65535	6/6	HTTP port.
alternateport	1025~65535	6/6	Alternate HTTP port.
authmode	basic, digest	1/6	HTTP authentication mode.
s0_accessname	string[32]	1/6	HTTP server push access name for stream 1. (capability.protocol.spush_mjpeg =1 and video.stream.count>0)
s1_accessname	string[32]	1/6	HTTP server push access name for stream 2. (capability.protocol.spush_mjpeg =1 and video.stream.count>1)
s2_accessname	string[32]	1/6	Http server push access name for stream 3 (capability.protocol.spush_mjpeg =1 and video.stream.count>2)
s3_accessname	string[32]	1/6	Http server push access name for stream 4 (capability.protocol.spush_mjpeg =1 and video.stream.count>3)

s4_accessname	string[32]	1/6	Http server push access name for stream 5 (capability.protocol.spush_mjpeg =1 and video.stream.count>4)
anonymousviewing	<boolean>	1/6	Enable anoymous streaming viewing.

5.6.6 HTTPS Port

Subgroup of network: https_port

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
port	443, 1025 ~ 65535	6/6	HTTPS port.

5.6.7 RTSP

Subgroup of **network**: **rtsp**

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
port	554, 1025 ~ 65535	1/6	RTSP port. (capability.protocol.rtsp=1)
anonymousviewing	<boolean>	1/6	Enable anoymous streaming viewing.
authmode	disable, basic, digest	1/6	RTSP authentication mode. (capability.protocol.rtsp=1)
s0_accessname	string[32]	1/6	RTSP access name for stream1. (capability.protocol.rtsp=1 and video.stream.count>0)
s1_accessname	string[32]	1/6	RTSP access name for stream2. (capability.protocol.rtsp=1 and video.stream.count>1)
s2_accessname	string[32]	1/6	RTSP access name for stream3 (capability.protocol.rtsp=1 and video.stream.count>2)
s3_accessname	string[32]	1/6	RTSP access name for stream4 (capability.protocol.rtsp=1 and video.stream.count>3)
S4_accessname	string[32]	1/6	RTSP access name for stream5 (capability.protocol.rtsp=1 and video.stream.count>4)
s0_audiotrack	<integer>	6/6	The current audio track for stream1. -1 => audio mute

s1_audiotrack	<integer>	6/6	The current audio track for stream2. -1 => audio mute

5.6.7.1 RTSP Multicast

Subgroup of **network_rtsp_s<0~(n-1)>**: **multicast,** n is stream count

(capability.protocol.rtp.multicast=1)

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
alwaysmulticast	<boolean>	4/4	Enable always multicast.
ipaddress	<ip address>	4/4	Multicast IP address.
videoport	1025 ~ 65535	4/4	Multicast video port.
audioport	1025 ~ 65535	4/4	Multicast audio port.
ttl	1 ~ 255	4/4	Multicast time to live value.

5.6.8 SIP Port

Subgroup of **network**: **sip**

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
Port	1025 ~ 65535	1/6	SIP port. (capability.protocol.sip=1)

5.6.9 RTP Port

Subgroup of **network**: **rtp**

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
videoport	1025 ~ 65535	6/6	Video channel port for RTP. (capability.protocol.rtp_unicast=1)
audioport	1025 ~ 65535	6/6	Audio channel port for RTP. (capability.protocol.rtp_unicast=1)

5.6.10 PPPoE

Subgroup of **network**: **pppoe**

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
user	string[128]	6/6	PPPoE account user name.
pass	password[64]	6/6	PPPoE account password.

5.7 IP Filter

Group: ipfilter

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
enable	<boolean>	6/6	Enable access list filtering.
admin_enable	<boolean>	6/6	Enable administrator IP address.
admin_ip	String[44]	6/6	Administrator IP address.
maxconnection	1~10	6/6	Maximum number of concurrent streaming connection(s).
allow_i<0~9>_start	1.0.0.0 ~ 255.255.255.255	6/6	Allowed starting IPv4 address for connection.
allow_i<0~9>_end	1.0.0.0 ~ 255.255.255.255	6/6	Allowed ending IPv4 address for connection.
deny_i<0~9>_start	1.0.0.0 ~ 255.255.255.255	6/6	Denied starting IPv4 address for connection.
deny_i<0~9>_end	1.0.0.0 ~ 255.255.255.255	6/6	Denied ending IPv4 address for connection.
ipv6_allow_i<0~9>	String[44]	6/6	Allowed IPv6 address for connection.
ipv6_deny_i<0~9>	String[44]	6/6	Denied IPv6 address for connection.

5.8 Video Input

Group: **videoin**

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
cmosfreq	50, 60	4/4	CMOS frequency. (videoin.type=2) (product dependent)
whitebalance	auto, manual	4/4	"auto" indicates auto white balance. "manual" indicates keep current value.
atwbvalue1	0 ~ 9999999999	4/4	The auto white balance value.
atwbvalue2	0 ~ 9999999999	4/4	The auto white balance value.
exposurelevel	1~8	4/4	Exposure level (product dependent)
irismode	fixed, indoor, outdoor	4/4	Video Iris or DC Iris. (product dependent)
irislevel	1 ~ 8	4/4	Iris level when connected to auto iris lens: 1 => brightest 8 => darkest (product dependent)
autoiris	<boolean>	4/4	Enable auto Iris. (product dependent)

enableblc	<boolean>	4/4	Enable backlight compensation. (product dependent)
agc	0~2	4/4	Max gain: 0->2x 1->4x 2->8x (product dependent)

5.8.1 Video Input Setting per Channel

Group: **videoin_c<0~(n-1)>** for n channel products, and m is stream number

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
color	0, 1	4/4	0 =>monochrome 1 => color
flip	<boolean>	4/4	Flip the image.
mirror	<boolean>	4/4	Mirror the image.
ptzstatus	<integer>	1/7	A 32-bit integer, each bit can be set separately as follows: Bit 0 => Support camera control function; 0(not support), 1(support) Bit 1 => **Built-in** or **external** camera; 0 (external), 1(built-in) Bit 2 => Support **pan** operation; 0(not support), 1(support) Bit 3 => Support **tilt** operation; 0(not support), 1(support) Bit 4 => Support **zoom** operation; 0(not support), 1(support) Bit 5 => Support **focus** operation; 0(not support), 1(support)
text	string[16]	1/4	Enclose caption.
imprinttimestamp	<boolean>	4/4	Overlay time stamp on video.
maxexposure	1~120	4/4	Maximum exposure time.
options	quality, framerate, crop	4/4	Customize video quality first or video frame rate first. (product dependent)
crop_position	<coordinate> (x,y)	1/4	Crop left-top corner coordinate.
crop_size	<window size> (WxH)	1/4	Crop width and height. (width must be 16x and height must be 8x)
s<0~(m-1)>_codect	mpeg4, mjpeg	1/4	Video codec type.

ype			
s<0~(m-1)>_resolution	2M CMOS => 176x144, 320x240, 640x480, 800x600, 1280x960, 1600x1200	1/4	Video resolution in pixels.
s<0~(m-1)>_mpeg4_intraperiod	250, 500, 1000, 2000, 3000, 4000	4/4	Intra frame period in milliseconds.
s<0~(m-1)>_mpeg4_ratecontrolmode	cbr, vbr	4/4	cbr, constant bitrate vbr, fix quality
s<0~(m-1)>_mpeg4_quant	0, 1~5	4/4	Quality of video when choosing vbr in "ratecontrolmode". 0 is the customized manual input setting. 1 = worst quality, 5 = best quality.
s<0~(m-1)>_mpeg4_bitrate	1000~8000000	4/4	Set bit rate in bps when choosing cbr in "ratecontrolmode".
s<0~(m-1)>_mpeg4_maxframe	1~30	1/4	Set maximum frame rate in fps (for MPEG-4).
s<0~(m-1)>_mpeg4_qvalue	1~31	4/4	Manual video quality level input - choose customize input "mpeg4_quant = 0" (for MPEG-4).
s<0~(m-1)>_mjpeg_quant	0 ~ 5	4/4	Quality of JPEG video. 0 is the customized manual input setting. 1 = worst quality, 5 = best quality.
s<0~(m-1)>_mjpeg_maxframe	1~30	1/4	Set maximum frame rate in fps (for JPEG).
s<0~(m-1)>_mjpeg_qvalue	10~200	4/4	Manual video quality level input - choose customize input "mjpeg_quant = 0" (for MJPEG).
s<0~(m-1)>_forcei	1	7/6	Force I frame.

5.8.1.1 Alternative Video Input Profiles per Channel

In addition to the primary setting of video input, there can be alternative profile video input setting for each channel which might be for different scene of light (daytime or nighttime).

Group: videoin_profile_i<0~(m-1)>

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
enable	<boolean>	4/4	Enable/disable this profile setting
policy	day, night, schedule	4/4	The mode which the profile is applied to.
begintime	hh:mm	4/4	Begin time of schedule mode.
endtime	hh:mm	4/4	End time of schedule mode.
autoiris	<boolean>	4/4	Enable auto Iris. (product dependent)
exposurelevel	1~8	4/4	Exposure level (product dependent)
maxexposure	1~120	4/4	Maximum exposure time.
agc	0~2	4/4	Max gain: 0->2x 1->4x 2->8x (product dependent)
enableblc	<boolean>	4/4	Enable backlight compensation. (product dependent)

5.9 Video Input Preview

The temporary setting for preview video.

Group: videoinpreview

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
autoiris	<boolean>	4/4	Preview of enable auto Iris. (product dependent)
enableblc	<boolean>	4/4	Preview of enable backlight compensation. (product dependent)
agc	0~2	4/4	Max gain: 0->2x 1->4x 2->8x (product dependent)
exposurelevel	1~8	4/4	Preview of exposure level (product dependent)
maxexposure	1~120	4/4	Maximum exposure time.

5.10 IR Cut Control

Group: ircutcontrol

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
mode	auto, day, night, di, schedule	6/6	Set IR cut control mode
daymodebegintime	00:00~23:59	6/6	Day mode begin time
daymodeendtime	00:00~23:59	6/6	Day mod end time
disableirled	<boolean>	6/6	Enable/disable IR led
bwmode	<boolean>	6/6	Switch to B/W in night mode if enabled
sensitivity	low, normal, high	6/6	Sensitivity of light sensor

5.11 Image Setting per Channel

Group: **image_c<0~(n-1)>** for n channel products

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
brightness	<product dependent>	4/4	Adjust brightness of image according to mode settings.
saturation	-5 ~ 5	4/4	Adjust saturation of image according to mode settings.
contrast	-5 ~ 5	4/4	Adjust contrast of image according to mode settings.
sharpness	<product dependent>	4/4	Adjust sharpness of image according to mode settings.
IBPE_edgeenable	<boolean>	4/4	Enable edge enhancement.(Haydn only)
IBPE_edgestrength	1 ~ 128	4/4	Adjust edge enhancement strength. 1 is minimum and 128 is maximum. (Haydn only)
IBPE_nrenable	<boolean>	4/4	Enable noise reduction. (Haydn only)
IBPE_nrmode	1 ~ 3	4/4	Adjust noise reduction mode. 1 => DeGaussian 2 => DeImpulse 3 => DeGaussian + DeImpulse (Haydn only)
IBPE_nrstrength	1 ~ 63	4/4	Adjust noise reduction strength. 1 is minimum and 63 is maximum. (Haydn only)

5.12 Image Setting for Preview

Group: **imagepreview_c<0~(n-1)>** for n channel products

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
brightness	<product dependent>	4/4	Preview of brightness adjustment of image according to mode settings.
saturation	-5 ~ 5	4/4	Preview of saturation adjustment of image according to mode settings.
contrast	-5 ~ 5	4/4	Preview of contrast adjustment of image according to mode settings.
sharpness	<product dependent>	4/4	Preview of sharpness adjustment of image according to mode settings.
IBPE_edgeenable	<boolean>	4/4	Preview of adjusting enabling edge enhancement. (Haydn only)
IBPE_edgestrength	1 ~ 128	4/4	Preview of adjusting edge enhancement strength. 1 is minimum and 128 is maximum. (Haydn only)
IBPE_nrenable	<boolean>	4/4	Preview of adjusting enabling noise reduction. (Haydn only)
IBPE_nrmode	1 ~ 3	4/4	Preview of adjusting noise reduction mode. 1 => DeGaussian 2 => DeImpulse 3 => DeGaussian + DeImpulse (Haydn only)
IBPE_nrstrength	1 ~ 63	4/4	Preview of adjusting noise reduction strength. 1 is minimum and 63 is maximum. (Haydn only)

Group: imagepreview

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
videoin_whitebalance	auto, manual	4/4	Preview of adjusting white balance of image according to mode settings
videoin_restoreatwb	0, 1~	4/4	Restore of adjusting white balance of image according to mode settings

5.13 Audio Input per Channel

Group: **audioin_c<0~(n-1)>** for n channel products (capability.audioin>0)

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
mute	0, 1	4/4	Enable audio mute.
gain	0~31	4/4	Gain of input.
s<0~(m-1)>_codectype	gamr	4/4	Set audio codec type for input.
s<0~(m-1)>_aac4_bitrate	16000, 32000, 48000, 64000, 96000, 128000	4/4	Set AAC4 bitrate in bps.
s<0~(m-1)>_gamr_bitrate	4750, 5150, 5900, 6700, 7400, 7950, 10200, 12200	4/4	Set AMR bitrate in bps.

5.14 Time Shift Settings

Group: **timeshift**, c for n channel products, m is stream number

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
enable	<boolean>	4/4	Enable time shift streaming.
c<0~(n-1)>_s<0~(m-1)>_allow	<boolean>	4/4	Enable time shift streaming for specific stream. (product dependent)

5.15 Motion Detection Settings

Group: **motion_c<0~(n-1)>** for m profile and n channel product

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
enable	<boolean>	4/4	Enable motion detection.
win_i<0~2>_enable	<boolean>	4/4	Enable motion window 1~3.
win_i<0~2>_name	string[14]	4/4	Name of motion window 1~3.
win_i<0~2>_left	0 ~ 320	4/4	Left coordinate of window position.
win_i<0~2>_top	0 ~ 240	4/4	Top coordinate of window position.
win_i<0~2>_width	0 ~ 320	4/4	Width of motion detection window.
win_i<0~2>_height	0 ~ 240	4/4	Height of motion detection window.
win_i<0~2>_objsize	0 ~ 100	4/4	Percent of motion detection window.
win_i<0~2>_sensitivity	0 ~ 100	4/4	Sensitivity of motion detection window.
profile_i<0~(m-1)>_enable	<boolean>	4/4	Enable profile 1 ~ (m-1).

profile_i<0~(m-1)>_policy	day, night, schedule	4/4	The mode which the profile is applied to.
profile_i<0~(m-1)>_begintime	hh:mm	4/4	Begin time of schedule mode.
profile_i<0~(m-1)>_endtime	hh:mm	4/4	End time of schedule mode.
profile_i<0~(m-1)>_win_i<0~2>_enable	<boolean>	4/4	Enable motion window.
profile_i<0~(m-1)>_win_i<0~2>_name	string[14]	4/4	Name of motion window.
profile_i<0~(m-1)>_win_i<0~2>_left	0 ~ 320	4/4	Left coordinate of window position.
profile_i<0~(m-1)>_win_i<0~2>_top	0 ~ 240	4/4	Top coordinate of window position.
profile_i<0~(m-1)>_win_i<0~2>_width	0 ~ 320	4/4	Width of motion detection window.
profile_i<0~(m-1)>_win_i<0~2>_height	0 ~ 240	4/4	Height of motion detection window.
profile_i<0~(m-1)>_win_i<0~2>_objsize	0 ~ 100	4/4	Percent of motion detection window.
profile_i<0~(m-1)>_win_i<0~2>_sensitivity	0 ~ 100	4/4	Sensitivity of motion detection window.

5.16 Tempering Detection Settings

Group: **tampering_c<0~(n-1)>** for n channel product

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
enable	<boolean>	4/4	Enable or disable tamper detection.
threshold	0 ~ 255	4/4	Threshold of tamper detection.
duration	10 ~ 600	4/4	If tampering value exceeds the 'threshold' for more than 'duration', then tamper detection is triggered.

5.17 DDNS

Group: **ddns**

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
enable	<boolean>	6/6	Enable or disable the dynamic DNS.
provider	Safe100, DyndnsDynamic, DyndnsCustom, TZO, DHS, DynInterfree, CustomSafe100	6/6	Safe100 => safe100.net DyndnsDynamic => dyndns.org (dynamic) DyndnsCustom => dyndns.org (custom) TZO => tzo.com DHS => dhs.org DynInterfree =>dyn-interfree.it

			CustomSafe100 => Custom server using safe100 method
<provider>_hostname	string[128]	6/6	Your dynamic hostname.
<provider>_username email	string[64]	6/6	Your user or email to login to the DDNS service provider
<provider>_password key	string[64]	6/6	Your password or key to login to the DDNS service provider.
<provider>_servername	string[128]	6/6	The server name for safe100. (This field only exists if the provider is customsafe100)

5.18 UPnP Presentation

Group: upnppresentation

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
enable	<boolean>	6/6	Enable or disable the UPNP presentation service.

5.19 UPnP Port Forwarding

Group: upnpportforwarding

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
enable	<boolean>	6/6	Enable or disable the UPNP port forwarding service.
upnpnatstatus	0~3	6/7	The status of UpnP port forwarding, used internally. 0 = OK, 1 = FAIL, 2 = no IGD router, 3 = no need for port forwarding

5.20 System Log

Group: **syslog**

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
enableremotelog	<boolean>	6/6	Enable remote log.
serverip	<IP address>	6/6	Log server IP address.
serverport	514, 1025~65535	6/6	Server port used for log.
level	0~7	6/6	Levels used to distinguish the importance of the information: 0: LOG_EMERG 1: LOG_ALERT 2: LOG_CRIT

			3: LOG_ERR 4: LOG_WARNING 5: LOG_NOTICE 6: LOG_INFO 7: LOG_DEBUG

5.21 Camera PTZ Control

Group: **camctrl** (product dependent)

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
enablehttptunnel	<boolean>	4/4	Enable HTTP tunnel for camera control.

Group: **camctrl_c<0~(n-1)>** for n channel product (capability.ptzenabled)

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
panspeed	-5 ~ 5	1/4	Pan speed
tiltspeed	-5 ~ 5	1/4	Tilt speed
zoomspeed	-5 ~ 5	1/4	Zoom speed
autospeed	-5 ~ 5	1/4	Auto pan speed
focusspeed	-5 ~ 5	1/4	Auto focus speed
preset_i<0~(npreset-1)>_name	string[40]	1/4	Name of the preset location.
uart	0 ~ (m-1), m is UART count	1/4	Select corresponding uart (capability.nuart>0).
cameraid	0~255	1/4	Camera ID controlling external PTZ camera.
isptz	0 ~ 2	1/7	0: disable PTZ commands. 1: enable PTZ commands with PTZ driver. 2: enable PTZ commands with UART tunnel.
disablemdonptz	<boolean>	1/4	Disable motion detection on PTZ operation.
patrolseq	string[64]	1/4	(For external device) The indexes of patrol points, separated by ",”
patroldwelling	string[128]	1/4	(For external device) The dwelling time of each patrol point, separated by ",”

5.22 UART Control

Group: **uart** (capability.nuart>0) (product dependent)

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
ptzdrivers_i<0~19, 127>_name	string[40]	1/4	Name of the PTZ driver.
ptzdrivers_i<0~19, 127>_location	string[128]	1/4	Full path of the PTZ driver.
enablehttptunnel	<boolean>	4/4	Enable HTTP tunnel channel to control UART.

Group: **uart_i<0~(n-1)>** n is uart port count (capability.nuart>0)

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
baudrate	110,300,600,1200,2400,3600,4800,7200,9600,19200,38400,57600,115200	4/4	Set baud rate of COM port.
databit	5,6,7,8	4/4	Data bits in a character frame.
paritybit	none, odd, even	4/4	For error checking.
stopbit	1,2	4/4	1 2-1.5 , data bit is 5 2-2
uartmode	rs485, rs232	4/4	RS485 or RS232.
customdrvcmd_i<0~9>	string[128]	1/4	PTZ command for custom camera.
speedlink_i<0~4>_name	string[40]	1/4	Additional PTZ command name.
speedlink_i<0~4>_cmd	string[128]	1/4	Additional PTZ command list.
ptzdriver	0~19, 127 (custom), 128 (no driver)	4/4	The PTZ driver is used by this COM port.

5.23 SNMP

Group: **snmp** (capability.snmp) (product dependent)

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
v2	0~1	6/6	SNMP v2 enabled. 0 for disable, 1 for enable
v3	0~1	6/6	SNMP v3 enabled. 0 for disable, 1 for enable
secnamerw	string[31]	6/6	Read/write security name
secnamero	string[31]	6/6	Read only security name
authpwrw	string[8~128]	6/6	Read/write authentication password

authpwro	string[8~128]	6/6	Read only authentication password
authtyperw	MD5,SHA	6/6	Read/write authentication type
authtypero	MD5,SHA	6/6	Read only authentication type
encryptpwrw	string[8~128]	6/6	Read/write password
encryptpwro	string[8~128]	6/6	Read only password
encrypttyperw	DES	6/6	Read/write encryption type
encrypttypero	DES	6/6	Read only encryption type
rwcommunity	string[31]	6/6	Read/write community
rocommunity	string[31]	6/6	Ready only community

5.24 Layout Configuration

Group: **layout** (product dependent) (FD7132)

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
logo_default	<boolean>	1/6	0 => Custom logo 1 => Default logo
logo_link	string[40]	1/6	Hyperlink of the logo
logo_powerbyvvtk_hidden	<boolean>	1/6	0 => display the power by vivotek logo 1 => hide the power by vivotek logo
theme_option	1~4	1/6	1~3: One of the default themes. 4: Custom definition.
theme_color_font	string[7]	1/6	Font color
theme_color_configfont	string[7]	1/6	Font color of configuration area.
theme_color_titlefont	string[7]	1/6	Font color of video title.
theme_color_controlbackground	string[7]	1/6	Background color of control area.
theme_color_configbackground	string[7]	1/6	Background color of configuration area.
theme_color_videobackground	string[7]	1/6	Background color of video area.
theme_color_case	string[7]	1/6	Frame color

5.25 Privacy Mask

Group: **privacymask_c<0~(n-1)>** for n channel product

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
enable	<boolean>	4/4	Enable privacy mask.
win_i<0~4>_enable	<boolean>	4/4	Enable privacy mask window.
win_i<0~4>_name	string[14]	4/4	Name of the privacy mask window.

win_i<0~4>_left	0 ~ 320/352	4/4	Left coordinate of window position.
win_i<0~4>_top	0 ~ 240/288	4/4	Top coordinate of window position.
win_i<0~4>_width	0 ~ 320/352	4/4	Width of privacy mask window.
win_i<0~4>_height	0 ~ 240/288	4/4	Height of privacy mask window.

5.26 Capability

Group: capability

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
api_httpversion	0100a	0/7	The HTTP API version.
bootuptime	<positive integer>	0/7	Server bootup time.
nir	0, <positive integer>	0/7	Number of IR interfaces.
ndi	0, <positive integer>	0/7	Number of digital inputs.
ndo	0, <positive integer>	0/7	Number of digital outputs.
naudioin	0, <positive integer>	0/7	Number of audio inputs.
naudioout	0, <positive integer>	0/7	Number of audio outputs.
nvideoin	<positive integer>	0/7	Number of video inputs.
nmediastream	<positive integer>	0/7	Number of media stream per channels.
nvideosetting	<positive integer>	0/7	Number of video settings per channel.
naudiosetting	<positive integer>	0/7	Number of audio settings per channel.
nuart	0, <positive integer>	0/7	Number of UART interfaces.
nmotionprofile	<positive integer>	0/7	Number of motion profiles.
ptzenabled	<positive integer>	0/7	An 32-bit integer, each bit can be set separately as follows: Bit 0 => Support camera control function; 0(not support), 1(support) Bit 1 => Built-in or external camera; 0(external), 1(built-in) Bit 2 => Support pan operation, 0(not support), 1(support) Bit 3 => Support tilt operation; 0(not support), 1(support) Bit 4 => Support zoom operation; 0(not support), 1(support) Bit 5 => Support focus operation; 0(not support), 1(support) Bit 6 => Support iris operation; 0(not support), 1(support)

			Bit 7 => External or built-in PT; (built-in), 1(external) Bit 8 => Invalidate bit 1 ~ 7; 0(bit 1 ~ 7 are valid), 1(bit 1 ~ 7 are invalid) Bit 9 => Reserved bit; Invalidate lens_pan, Lens_tilt, lens_zoon, lens_focus, len_iris. 0(fields are valid), 1(fields are invalid)
eptz	<positive integer>	0/7	A 32-bit integer, each bit can be set separately as follows: Bit 0 => stream 1 supports ePTZ or not. Bit 1 => stream 2 supports ePTZ or not. The rest may be deduced by analogy
npreset	<positive integer>	0/7	Number of preset locations.
protocol_https	< boolean >	0/7	Indicate whether to support HTTP over SSL.
protocol_rtsp	< boolean >	0/7	Indicate whether to support RTSP.
protocol_sip	<boolean>	0/7	Indicate whether to support SIP.
protocol_maxconnection	<positive integer>	0/7	The maximum allowed simultaneous connections.
protocol_rtp_multicast_scalable	<boolean>	0/7	Indicate whether to support scalable multicast.
protocol_rtp_multicast_backchannel	<boolean>	0/7	Indicate whether to support backchannel multicast.
protocol_rtp_tcp	<boolean>	0/7	Indicate whether to support RTP over TCP.
protocol_rtp_http	<boolean>	0/7	Indicate whether to support RTP over HTTP.
protocol_spush_mjpeg	<boolean>	0/7	Indicate whether to support server push MJPEG.
protocol_snmp	<boolean>	0/7	Indicate whether to support SNMP.
protocol_ipv6	<boolean>	0/7	Indicate whether to support IPv6.
videoin_type	0, 1, 2	0/7	0 => Interlaced CCD 1 => Progressive CCD 2 => CMOS
videoin_resolution	<a list of available resolution separated by commas>	0/7	Available resolutions list.
videoin_maxframerate	<a list of available maximum frame rate separated by commas>	0/7	Available maximum frame list.

videoin_codec	<a list of available codec types separated by commas>	0/7	Available codec list.
videoout_codec	<a list of the available codec types separated by commas)	0/7	Available codec list.
audio_aec	<boolean>	0/7	Indicate whether to support acoustic echo cancellation.
audio_extmic	<boolean>	0/7	Indicate whether to support external microphone input.
audio_linein	<boolean>	0/7	Indicate whether to support external line input.
audio_lineout	<boolean>	0/7	Indicate whether to support line output.
audio_headphoneout	<boolean>	0/7	Indicate whether to support headphone output.
audioin_codec	<a list of the available codec types separated by commas)	0/7	Available codec list.
audioout_codec	<a list of the available codec types separated by commas)	0/7	Available codec list.
uart_httptunnel	<boolean>	0/7	Indicate whether to support HTTP tunnel for UART transfer.
camctrl_privilege	<boolean>	0/7	Indicate whether to support "Manage Privilege" of PTZ control in the Security page.
transmission_mode	Tx, Rx, Both	0/7	Indicate transmission mode of the machine: TX = server, Rx = receiver box, Both = DVR.
network_wire	<boolean>	0/7	Indicate whether to support Ethernet.
network_wireless	<boolean>	0/7	Indicate whether to support wireless.
wireless_s802dot11b	<boolean>	0/7	Indicate whether to support wireless 802.11b+.
wireless_s802dot11g	<boolean>	0/7	Indicate whether to support wireless 802.11g.
wireless_beginchanne	1 ~ 14	0/7	Indicate the begin channel of wireless

l			network
wireless_endchannel	1 ~ 14	0/7	Indicate the end channel of wireless network
wireless_encrypt_wep	<boolean>	0/7	Indicate whether to support wireless WEP.
wireless_encrypt_wpa	<boolean>	0/7	Indicate whether to support wireless WPA.
wireless_encrypt_wpa2	<boolean>	0/7	Indicate whether to support wireless WPA2.
derivative_brand	<boolean>	0/7	Indicate whether to support the upgrade function for the derivative brand. For example, if the value is true, the VVTK product can be upgraded to VVXX. (TCVV<->TCXX is excepted)
evctrlchannel	<boolean>	0/7	Indicate whether to support HTTP tunnel for event/control transfer.
joystick	<boolean>	0/7	Indicate whether to support joystick control.
nanystream	<positive integer>	0/7	number of any media stream per channel
ir	<boolean>	0/7	Indicate whether to support IR led.

5.27 Customized Event Script

Group: event_customtaskfile_i<0~2>

PARAMETER	VALUE	SECURITY (get/set)	DESCRIPTION
name	string[41]	6/6	Custom script identification of this entry.
date	string[17]	6/6	Date of custom script.
time	string[17]	6/6	Time of custom script.

5.28 Event Setting

Group: **event_i**<0~2>

PARAMETER	VALUE	SECURITY (get/set)	DESCRIPTION
name	string[40]	6/6	Identification of this entry.
enable	0, 1	6/6	Enable or disable this event.
priority	0, 1, 2	6/6	Indicate the priority of this event: "0" = low priority "1" = normal priority "2" = high priority
delay	1~999	6/6	Delay in seconds before detecting the next event.

trigger	boot, di, motion, seq, visignal, pir, recnotify, audioswitch, tampering, iva	6/6	Indicate the trigger condition: "boot" = System boot "di"= Digital input "motion" = Video motion detection "seq" = Periodic condition "visignal" = Video input signal loss. "pir" = PIR detection. "recnotify" = Recording notification. "audioswitch" = Audio switch. "tampering" = Tamper detection. "iva" = IVA trigger.
triggerstatus	String[40]	6/6	The status for event trigger
di	<integer>	6/6	Indicate which DI detects. This field is required when trigger condition is "di". One bit represents one digital input. The LSB indicates DI 0.
mdwin	<integer>	6/6	Indicate which motion detection windows detect. This field is required when trigger condition is "md". One bit represents one window. The LSB indicates the 1st window. For example, to detect the 1st and 3rd windows, set mdwin as 5.
mdwin0	<integer>	6/6	Indicate which motion detection windows of profile 1 detect.
inter	1~999	6/6	Interval of snapshots in minutes. This field is used when trigger condition is "seq".
weekday	0~127	6/6	Indicate which weekday is scheduled. One bit represents one weekday. bit0 (LSB) = Saturday bit1 = Friday bit2 = Thursday bit3 = Wednesday bit4 = Tuesday bit5 = Monday bit6 = Sunday For example, to detect events on Friday and Sunday, set weekday as 66.
begintime	hh:mm	6/6	Begin time of the weekly schedule.
endtime	hh:mm	6/6	End time of the weekly schedule. (00:00 ~ 24:00 sets schedule as always on)

lowlightcondition	0, 1	6/6	0 => Do action at all times 1 => Do action in low-light conditions
action_do_i<0~(ndo-1)>_enable	0, 1	6/6	Enable or disable trigger digital output.
action_do_i<0~(ndo-1)>_duration	1~999	6/6	Duration of the digital output trigger in seconds.
action_cf_enable	0. 1	6/6	Enable media write on CF.
action_cf_folder	string[128]	6/6	Path to store media.
action_cf_media	NULL, 0~4	6/6	Index of the attached media.
action_cf_datefolder	<boolean>	6/6	Enable this to create folders by date, time, and hour automatically.
action_server_i<0~4>_enable	0, 1	6/6	Enable or disable this server action. The default value is 0.
action_server_i<0~4>_media	NULL, 0~4	6/6	Index of the attached media.
action_server_i<0~4>_datefolder	<boolean>	6/6	Enable this to create folders by date, time, and hour automatically.
action_goto_enable	<Boolean>	6/6	Enable/disable ptz goto preset on event triggered.
action_goto_name	string[40]	6/6	Preset name that ptz goto on event triggered.

5.29 Server Setting for Event Action

Group: **server_i**<0~4>

PARAMETER	VALUE	SECURITY (get/set)	DESCRIPTION
name	string[40]	6/6	Identification of this entry
type	email, ftp, http, ns	6/6	Indicate the server type: "email" = email server "ftp" = FTP server "http" = HTTP server "ns" = network storage
http_url	string[128]	6/6	URL of the HTTP server to upload.
http_username	string[64]	6/6	Username to log in to the server.
http_passwd	string[64]	6/6	Password of the user.
ftp_address	string[128]	6/6	FTP server address.
ftp_username	string[64]	6/6	Username to log in to the server.
ftp_passwd	string[64]	6/6	Password of the user.
ftp_port	0~65535	6/6	Port to connect to the server.
ftp_location	string[128]	6/6	Location to upload or store the media.

ftp_passive	0, 1	6/6	Enable or disable passive mode. 0 = disable passive mode 1 = enable passive mode
email_address	string[128]	6/6	Email server address.
email_sslmode	0, 1	6/6	Enable support SSL.
email_port	0~65535	6/6	Port to connect to the server.
email_username	string[64]	6/6	Username to log in to the server.
email_passwd	string[64]	6/6	Password of the user.
email_senderemail	string[128]	6/6	Email address of the sender.
email_recipientemail	string[128]	6/6	Email address of the recipient.
ns_location	string[128]	6/6	Location to upload or store the media.
ns_username	string[64]	6/6	Username to log in to the server.
ns_passwd	string[64]	6/6	Password of the user.
ns_workgroup	string[64]	6/6	Workgroup for network storage.

5.30 Media Setting for Event Action

Group: **media_i<0~4>** (media_freespace is used internally.)

PARAMETER	VALUE	SECURITY (get/set)	DESCRIPTION
name	string[40]	6/6	Identification of this entry
type	snapshot, systemlog, videoclip, recordmsg	6/6	Media type to send to the server or store on the server.
snapshot_source	<integer>	6/6	Indicate the source of media stream. 0 means the first stream. 1 means the second stream and etc. 2 means the third stream and etc. 3 means the fourth stream and etc.
snapshot_prefix	string[16]	6/6	Indicate the prefix of the filename.
snapshot_datesuffix	0, 1	6/6	Add date and time suffix to filename: 1 = Add date and time suffix. 0 = Do not add.
snapshot_preevent	0 ~ 7	6/6	Indicates the number of pre-event images.
snapshot_postevent	0 ~ 7	6/6	The number of post-event images.

videoclip_source	<integer>	6/6	Indicate the source of media stream. 0 means the first stream. 1 means the second stream and etc. 2 means the third stream and etc. 3 means the fourth stream and etc.
videoclip_prefix	string[16]	6/6	Indicate the prefix of the filename.
videoclip_preevent	0 ~ 9	6/6	Indicates the time for pre-event recording in seconds.
videoclip_maxduration	1 ~ 10	6/6	Maximum duration of one video clip in seconds.
videoclip_maxsize	50 ~ 1500	6/6	Maximum size of one video clip file in Kbytes.

5.31 Recording

Group: **recording_i**<0~1>

PARAMETER	VALUE	SECURITY (get/set)	DESCRIPTION
name	string[40]	6/6	Identification of this entry.
enable	0, 1	6/6	Enable or disable this recording.
priority	0, 1, 2	6/6	Indicate the priority of this recording: "0" indicates low priority. "1" indicates normal priority. "2" indicates high priority.
source	<integer>	6/6	Indicate the source of media stream. 0 means the first stream. 1 means the second stream and etc. 2 means the third stream and etc. 3 means the fourth stream and etc.
limitsize	0,1	6/6	0: Entire free space mechanism 1: Limit recording size mechanism
cyclic	0,1	6/6	0: Disable cyclic recording 1: Enable cyclic recording
notify	0,1	6/6	0: Disable recording notification 1: Enable recording notification

notifyserver	0~31	6/6	Indicate which notification server is scheduled.One bit represents one application server (server_i0~i4). bit0 (LSB) = server_i0. bit1 = server_i1. bit2 = server_i2. bit3 = server_i3. bit4 = server_i4. For example, enable server_i0, server_i2, and server_i4 as notification servers; the notifyserver value is 21.
weekday	0~127	6/6	Indicate which weekday is scheduled. One bit represents one weekday. bit0 (LSB) = Saturday bit1 = Friday bit2 = Thursday bit3 = Wednesday bit4 = Tuesday bit5 = Monday bit6 = Sunday For example, to detect events on Friday and Sunday, set weekday as 66.
begintime	hh:mm	6/6	Start time of the weekly schedule.
endtime	hh:mm	6/6	End time of the weekly schedule. (00:00~24:00 indicates schedule always on)
prefix	string[16]	6/6	Indicate the prefix of the filename.
cyclesize	20~	6/6	The maximum size for cycle recording in Kbytes when choosing to limit recording size.
reserveamount	15~	6/6	The reserved amount in Mbytes when choosing cyclic recording mechanism.
dest	cf, 0~4	6/6	The destination to store the recorded data. "cf" means CF card. "0~4" means the index of the network storage.
cffolder	string[128]	6/6	Folder name.

5.32 HTTPS

Group: **https** (product dependent)

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
connect	1025 ~ 65535	7/7	Specify the stunnel connect port.
enable	<boolean>	6/6	To enable or disable secure HTTP.

policy	<Boolean>	6/6	If the value is 1, it will force HTTP connection redirect to HTTPS connection
method	auto, manual, install	6/6	auto => Create self-signed certificate automatically. manual => Create self-signed certificate manually. install => Create certificate request and install.
status	-3 ~ 1	6/6	Specify the https status. -3 = Certificate not installed -2 = Invalid public key -1 = Waiting for certificate 0 = Not installed 1 = Active
countryname	string[2]	6/6	Country name in the certificate information.
stateorprovincename	string[128]	6/6	State or province name in the certificate information.
localityname	string[128]	6/6	The locality name in the certificate information.
organizationname	string[64]	6/6	Organization name in the certificate information.
unit	string[32]	6/6	Organizational unit name in the certificate information.
commonname	string[64]	6/6	Common name in the certificate information.
validdays	0 ~ 9999	6/6	Valid period for the certification.

5.33 Storage Management Setting

Currently it's for local storage (SD, CF card)

Group: **disk_i<0~(n-1)>** n is the total number of storage devices.

PARAMETER	VALUE	SECURITY (get/set)	DESCRIPTION
cyclic_enabled	<boolean>	6/6	Enable cyclic storage method.
autocleanup_enabled	<boolean>	6/6	Enable automatic clean up method. Expired and not locked media files will be deleted.
autocleanup_maxage	<positive integer>	6/6	To specify the expired days for automatic clean up.

5.34 Region of Interest

Group: **roi_c<0~(n-1)>** for n channel product, and m is the number of streams which support ROI.

PARAMETER	VALUE	SECURITY (get/set)	DESCRIPTION
s<0~(m-1>_home	<coordinate>	6/6	ROI left-top corner coordinate.

s<0~(m-1>_size	<window size>	6/6	ROI width and height. (width must be 16x and height must be 8x)

5.35 ePTZ Setting

Group: **eptz_c<0~(n-1)>** for n channel product.

PARAMETER	VALUE	SECURITY (get/set)	DESCRIPTION
osdzoom	<boolean>	1/4	Indicates multiple of zoom in is "on-screen display" or not
smooth	<boolean>	1/4	Indicates ePTZ is smooth or not.
tiltspeed	-5 ~ 5	1/7	Tilt speed (It should be set by eCamCtrl.cgi rather than by setparam.cgi.)
panspeed	-5 ~ 5	1/7	Pan speed (It should be set by eCamCtrl.cgi rather than by setparam.cgi.)
zoomspeed	-5 ~ 5	1/7	Zoom speed (It should be set by eCamCtrl.cgi rather than by setparam.cgi.)
autospeed	1 ~ 5	1/7	Auto pan/patrol speed (It should be set by eCamCtrl.cgi rather than by setparam.cgi.)

Group: **eptz_c<0~(n-1)>_s<0~(m-1)>** for n channel product. and m is the number of streams which support ePTZ.

PARAMETER	VALUE	SECURITY (get/set)	DESCRIPTION
patrolseq	string[120]	1/4	The indexes of patrol points, separated by ","
patroldwelling	string[160]	1/4	The dwelling time of each patrol point, separated by ","
i<0~19>_name	string[40]	1/7	Name of ePTZ preset. (It should be set by eCamCtrl.cgi rather than by setparam.cgi.)
i<0~19>_pos	<coordinate>	1/7	Left-top corner coordinate of the preset. (It should be set by eCamCtrl.cgi rather than by setparam.cgi.)
i<0~19>_size	<window size>	1/7	Width and height of the preset. (It should be set by eCamCtrl.cgi rather than by setparam.cgi.)

6. Useful Functions

6.1 Drive the Digital Output

Note: This request requires Viewer privileges.

Method: GET/POST

Syntax:

http://<*servername*>/cgi-bin/dido/setdo.cgi?do1=<*state*>[&do2=<state>]
[&do3=<state>][&do4=<state>][&return=<*return page*>]

Where state is 0 or 1; "0" means inactive or normal state, while "1" means active or triggered state.

PARAMETER	VALUE	DESCRIPTION
do<num>	0, 1	0 – Inactive, normal state
		1 – Active, triggered state
return	<*return page*>	Redirect to the page <*return page*> after the parameter is assigned. The <*return page*> can be a full URL path or relative path according to the current path. If you omit this parameter, it will redirect to an empty page.

Example: Drive the digital output 1 to triggered state and redirect to an empty page.

http://myserver/cgi-bin/dido/setdo.cgi?do1=1

6.2 Query Status of the Digital Input

Note: This request requires Viewer privileges

Method: GET/POST

Syntax:

http://<*servername*>/cgi-bin/dido/getdi.cgi?[di0][&di1][&di2][&di3]

If no parameter is specified, all of the digital input statuses will be returned.

Return:

HTTP/1.0 200 OK\r\n
Content-Type: text/plain\r\n
Content-Length: <*length*>\r\n
\r\n
[di0=<state>]\r\n
[di1=<state>]\r\n

[di2=<state>]\r\n
[di3=<state>]\r\n

where *<state>* can be 0 or 1.

Example: Query the status of digital input 1.

Request:
http://myserver/cgi-bin/dido/getdi.cgi?di1

Response:
HTTP/1.0 200 OK\r\n
Content-Type: text/plain\r\n
Content-Length: 7\r\n
\r\n
di1=1\r\n

6.3 Query Status of the Digital Output

Note: This request requires Viewer privileges

Method: GET/POST

Syntax:

http://*<servername>*/cgi-bin/dido/getdo.cgi?[do0][&do1][&do2][&do3]

If no parameter is specified, all the digital output statuses will be returned.

Return:

HTTP/1.0 200 OK\r\n
Content-Type: text/plain\r\n
Content-Length: *<length>*\r\n
\r\n
[do0=<state>]\r\n
[do1=<state>]\r\n
[do2=<state>]\r\n
[do3=<state>]\r\n

where *<state>* can be 0 or 1.

Example: Query the status of digital output 1.

Request:
http://myserver/cgi-bin/dido/getdo.cgi?do1

Response:

HTTP/1.0 200 OK\r\n

Content-Type: text/plain\r\n

Content-Length: 7\r\n

\r\n

do1=1\r\n

6.4 Drive the IR Light Illuminator

Note: This request requires Viewer privileges.

Method: GET/POST

Syntax:

http://<*servername*>/cgi-bin/dido/setilluminator.cgi?ir_status=<*state*>[&ir_duration=<value>]

Where state is close or open; "close" means inactive or normal state, while "open" means active or triggered state.

PARAMETER	VALUE	DESCRIPTION
ir_status	close, open	close– Inactive, normal state
		open– Active, triggered state
ir_duration	0~	Duration of the IR illuminator trigger in seconds.

Example: Drive the IR illuminator status to 1 and duration to 10 to triggered state for 10 seconds.

http://myserver/cgi-bin/dido/setilluminator.cgi?ir_status=open&ir_duration=10

6.5 Query Status of the IR Light Illuminator

Note: This request requires Viewer privileges

Method: GET/POST

Syntax:

http://<*servername*>/cgi-bin/dido/getilluminator.cgi?ir_status

If no parameter is specified, no result will be returned.

Return:

HTTP/1.0 200 OK\r\n

Content-Type: text/plain\r\n

[*ir_status*=<*state*>]\r\n

where <*state*> can be 0 or 1.

Example: Query the status of IR illuminator.

Request:

http://myserver/cgi-bin/dido/getilluminator.cgi?ir_status

Response:

HTTP/1.0 200 OK\r\n

Content-Type: text/plain\r\n

ir_status=1\r\n

6.6 Capture Single Snapshot

Note: This request requires Normal User privileges.

Method: GET/POST

Syntax:

http://<*servername*>/cgi-bin/viewer/video.jpg?[channel=<value>][&resolution=<value>]
[&quality=<value>][&streamid=<value>]

If the user requests a size larger than all stream settings on the server, this request will fail.

PARAMETER	VALUE	DESCRIPTION
channel	0~(n-1)	The channel number of the video source.
resolution	*<available resolution>*	The resolution of the image.
quality	*1~5*	The quality of the image.
Streamed <product dependent>	*0~(m-1)*	The stream number.

The server will return the most up-to-date snapshot of the selected channel and stream in JPEG format. The size and quality of the image will be set according to the video settings on the server.

Return:

HTTP/1.0 200 OK\r\n

Content-Type: image/jpeg\r\n

[Content-Length: <image size>\r\n]

<binary JPEG image data>

6.7 Account Management

Note: This request requires Administrator privileges.

Method: GET/POST

Syntax:

http://<*servername*>/cgi-bin/admin/editaccount.cgi?
method=<value>&username=<*name*>[&userpass=<*value*>][&privilege=<*value*>]
[&privilege=<value>][…][&return=<*return page*>]

PARAMETER	VALUE	DESCRIPTION
method	Add	Add an account to the server. When using this method, the "username" field is necessary. It will use the default value of other fields if not specified.
	Delete	Remove an account from the server. When using this method, the "username" field is necessary, and others are ignored.
	edit	Modify the account password and privilege. When using this method, the "username" field is necessary, and other fields are optional. If not specified, it will keep the original settings.
username	<name>	The name of the user to add, delete, or edit.
userpass	<value>	The password of the new user to add or that of the old user to modify. The default value is an empty string.
Privilege	<value>	The privilege of the user to add or to modify.
	viewer	Viewer privilege.
	operator	Operator privilege.
	admin	Administrator privilege.
Return	<return page>	Redirect to the page <*return page*> after the parameter is assigned. The <*return page*> can be a full URL path or relative path according to the current path. If you omit this parameter, it will redirect to an empty page.

6.8 System Logs

Note: This request requires Administrator privileges.

Method: GET/POST

Syntax:

http://<*servername*>/cgi-bin/admin/syslog.cgi

Server will return the most up-to-date system log.

Return:

```
HTTP/1.0 200 OK\r\n
Content-Type: text/plain\r\n
Content-Length: <syslog length>\r\n
\r\n
<system log information>\r\n
```

6.9 Configuration File (optional)

Note: This request requires Administrator privileges.

Method: GET/POST

Syntax:

```
http://<servername>/cgi-bin/admin/configfile.cgi?[format=<value>]
```

Server will return the most up-to-date configuration file.

PARAMETER	VALUE	DESCRIPTION
format	xml	Format for the config file.

Return:

```
HTTP/1.0 200 OK\r\n
Content-Type: text/plain\r\n
Content-Length: <configuration file length>\r\n
\r\n
<configuration data>\r\n
```

6.10 Upgrade Firmware

Note: This request requires Administrator privileges.

Method: POST

Syntax:

```
http://<servername>/cgi-bin/admin/upgrade.cgi
```

Post data:

```
fimage=<file name>[&return=<return page>]\r\n
\r\n
<multipart encoded form data>
```

Server will accept the file named <file name> to upgrade the firmware and return with <return page> if indicated.

6.11 Camera Control (capability.ptzenabled=1)

Note: This request requires Viewer privileges.

Method: GET/POST

Syntax:

http://<*servername*>/cgi-bin/viewer/camctrl.cgi?[channel=<value>][&camid=<value>][&move=<value>]
[&focus=<value>][&iris=<value>][&speedpan=<value>][&speedtilt=<value>][&speedzoom=<value>]
[&speedapp=<value>][&auto=<value>][&zoom=<value>][&zooming=<value>][&speedlink=<value>]
[&vx=<value>&vy=<value>&vs=<value>] [&return=<*return page*>]

PARAMETER	VALUE	DESCRIPTION
channel	<0~(n-1)>	Channel of video source.
camid	0,<positive integer>	Camera ID.
move	home	Move to camera to home position.
	up	Move camera up.
	down	Move camera down.
	left	Move camera left.
	right	Move camera right.
speedpan	-5 ~ 5	Set the pan speed.
speedtilt	-5 ~ 5	Set the tilt speed.
speedzoom	-5 ~ 5	Set the zoom speed.
speedfocus	-5 ~ 5	Set the focus speed.
speedapp	-5 ~ 5	Set the auto pan/patrol speed.
auto	pan	Auto pan.
	patrol	Auto patrol.
	stop	Stop camera.
zoom	wide	Zoom larger view with current speed.
	tele	Zoom further with current speed.
	stop	Stop zoom.
zooming	wide	Zoom without stopping for larger view with current speed.
	tele	Zoom without stopping for further view with current speed.
vx	<integer , excluding 0>	The slope of movement = vy/vx, used for joystick control.
vy	<integer>	
vs	0 ~ 7	Set the speed of movement, "0" means stop.

focus	auto	Auto focus.
	far	Focus on further distance.
	near	Focus on closer distance.
iris	auto	Let the Network Camera control iris size.
	open	Manually control the iris for bigger size.
	close	Manually control the iris for smaller size.
speedlink	0 ~ 4	Issue speed link command.
gaptime	0~32768	The gaptime between two consecutive ptz commands for device. (unit: ms)
return	<return page>	Redirect to the page *<return page>* after the parameter is assigned. The *<return page>* can be a full URL path or relative path according to the current path. If you omit this parameter, it will redirect to an empty page.

6.12 ePTZ Camera Control

Note: This request requires camctrl privileges.

Method: GET/POST

Syntax:

http://<*servername*>/cgi-bin/camctrl/eCamCtrl.cgi?channel=<value>&stream=<value>
[&move=<value>][&auto=<value>][&zoom=<value>]
[&zooming=<value>&zs=<value>]
[&vx=<value>&vy=<value>&vs=<value>]
[&speedpan=<value>][&speedtilt=<value>][&speedzoom=<value>][&speedapp=<value>]
[&return=<return page>]

PARAMETER	VALUE	DESCRIPTION
channel	<0~(n-1)>	Channel of video source.
stream	<0~(m-1)>	Stream.
move	home	Move to home ROI.
	up	Move up.
	down	Move down.
	left	Move left.
	right	Move right.
auto	pan	Auto pan.
	patrol	Auto patrol.
	stop	Stop auto pan/patrol.
zoom	wide	Zoom larger view with current speed.

	tele	Zoom further with current speed.
zooming	wide or tele	Zoom without stopping for larger view or further view with zs speed, used for joystick control.
zs	0 ~ 6	Set the speed of zooming, "0" means stop.
vx	<integer>	The direction of movement, used for joystick control.
vy	<integer>	
vs	0 ~ 7	Set the speed of movement, "0" means stop.
speedpan	-5 ~ 5	Set the pan speed.
speedtilt	-5 ~ 5	Set the tilt speed.
speedzoom	-5 ~ 5	Set the zoom speed.
speedapp	1 ~ 5	Set the auto pan/patrol speed.
return	<return page>	Redirect to the page <*return page*> after the parameter is assigned. The <*return page*> can be a full URL path or relative path according to the current path.

6.13 Recall (capability.ptzenabled=1)

Note: This request requires Viewer privileges.

Method: GET

Syntax:

http://<*servername*>/cgi-bin/viewer/recall.cgi?
recall=<value>[&channel=<value>][&return=<*return page*>]

PARAMETER	VALUE	DESCRIPTION
recall	Text string less than 30 characters	One of the present positions to recall.
channel	<0~(n-1)>	Channel of the video source.
return	<*return page*>	Redirect to the page <*return page*> after the parameter is assigned. The <*return page*> can be a full URL path or relative path according to the current path. If you omit this parameter, it will redirect to an empty page.

6.14 ePTZ Recall

Note: This request requires camctrl privileges.

Method: GET/POST

Syntax:

http://<*servername*>/cgi-bin/camctrl/eRecall.cgi?channel=<value>&stream=<value>&

recall=<value>[&return=<*return page*>]

PARAMETER	VALUE	DESCRIPTION
channel	<0~(n-1)>	Channel of the video source.
stream	<0~(m-1)>	Stream.
Recall	Text string less than 40 characters	One of the present positions to recall.
Return	<*return page*>	Redirect to the page <*return page*> after the parameter is assigned. The <*return page*> can be a full URL path or relative path according to the current path.

6.15 Preset Locations (capability.ptzenabled=1)

Note: This request requires Operator privileges.

Method: GET/POST

Syntax:

http://<*servername*>/cgi-bin/operator/preset.cgi?[channel=<value>] [&addpos=<value>][&delpos=<value>][&return=<*return page*>]

PARAMETER	VALUE	DESCRIPTION
addpos	<Text string less than 30 characters>	Add one preset location to the preset list.
channel	<0~(n-1)>	Channel of the video source.
delpos	<Text string less than 30 characters>	Delete preset location from preset list.
return	<*return page*>	Redirect to the page <*return page*> after the parameter is assigned. The <*return page*> can be a full URL path or relative path according to the current path. If you omit this parameter, it will redirect to an empty page.

6.16 ePTZ Preset Locations

Note: This request requires Operator privileges.

Method: GET/POST

Syntax:

http://<*servername*>/cgi-bin/operator/ePreset.cgi?channel=<value>&stream=<value>

[&addpos=<value>][&delpos=<value>][&return=<*return page*>]

PARAMETER	VALUE	DESCRIPTION
channel	<0~(n-1)>	Channel of the video source.
stream	<0~(m-1)>	Stream.
addpos	<Text string less than 40 characters>	Add one preset location to the preset list.
delpos	<Text string less than 40 characters>	Delete preset location from the preset list.
return	<*return page*>	Redirect to the page <*return page*> after the parameter is assigned. The <*return page*> can be a full URL path or relative path according to the current path.

6.17 IP Filtering

Note: This request requires Administrator access privileges.

Method: GET/POST

Syntax:

http://<*servername*>/cgi-bin/admin/ipfilter.cgi? method=<value>&[start=<*ipaddress*>&end=<*ipaddress*>][&index=<*value*>] [&return=<return page>]

PARAMETER	VALUE	DESCRIPTION
Method	addallow	Add allowed IP address range to the server. Start and end parameters must be specified. If the index parameter is specified, it will try to add starting from the index position.
	adddeny	Add denied IP address range to the server. Start and end parameters must be specified. If the index parameter is specified, it will try to add starting from the index position.
	deleteallow	Remove allowed IP address range from server. If start and end parameters are specified, it will try to remove the matched IP address. If index is specified, it will try to remove the address from given index position. [start, end] parameters have higher priority then the [index] parameter.
	deletedeny	Remove denied IP address range from server. If start and end parameters are specified, it will try to remove the matched IP address. If index is specified, it will try to remove the address from given index position. [start, end] parameters have higher priority then the [index] parameter.
start	<ip address>	The starting IP address to add or to delete.
end	<ip address>	The ending IP address to add or to delete.
index	<value>	The start position to add or to delete.

return	<return page>	Redirect to the page <*return page*> after the parameter is assigned. The <*return page*> can be a full URL path or relative path according to the current path. If you omit this parameter, it will redirect to an empty page.

6.18 UART HTTP Tunnel Channel (capability.nuart>0)

Note: This request requires Operator privileges.

Method: GET and POST

Syntax:

http://<*servername*>/cgi-bin/operator/uartchannel.cgi?[channel=<value>]

GET /cgi-bin/operator/uartchannel.cgi?[channel=<value>]

x-sessioncookie: string[22]

accept: application/x-vvtk-tunnelled

pragma: no-cache

cache-control: no-cache

POST /cgi-bin/operator/uartchannel.cgi

x-sessioncookie: string[22]

content-type: application/x-vvtk-tunnelled

pragma : no-cache

cache-control : no-cache

content-length: 32767

expires: Sun, 9 Jam 1972 00:00:00 GMT

User must use GET and POST to establish two channels for downstream and upstream. The x-sessioncookie in GET and POST should be the same to be recognized as a pair for one session. The contents of upstream should be base64 encoded to be able to pass through a proxy server.

This channel will help to transfer the raw data of UART over the network.

Please see UART tunnel spec for detail information

PARAMETER	VALUE	DESCRIPTION
channel	0 ~ (n-1)	The channel number of UART.

6.19 Event/Control HTTP Tunnel Channel

Note: This request requires Administrator privileges.

Method: GET and POST

Syntax:

```
http://<servername>/cgi-bin/admin/ctrlevent.cgi
---------------------------------------------------------------------------
GET /cgi-bin/admin/ctrlevent.cgi
x-sessioncookie: string[22]
accept: application/x-vvtk-tunnelled
pragma: no-cache
cache-control: no-cache


---------------------------------------------------------------------------
POST /cgi-bin/admin/ ctrlevent.cgi
x-sessioncookie: string[22]
content-type: application/x-vvtk-tunnelled
pragma : no-cache
cache-control : no-cache
content-length: 32767
expires: Sun, 9 Jam 1972 00:00:00 GMT
```

User must use GET and POST to establish two channels for downstream and upstream. The x-sessioncookie in GET and POST should be the same to be recognized as a pair for one session. The contents of upstream should be base64 encoded to be able to pass through the proxy server.

This channel will help perform real-time event subscription and notification as well as camera control more efficiently. The event and control formats are described in another document.

See Event/control tunnel spec for detail information

6.20 Get SDP of Streams

Note: This request requires Viewer access privileges.

Method: GET/POST

Syntax:

```
http://<servername>/<network_rtsp_s<0~m-1>_accessname>
```

"m" is the stream number.

"network_accessname_<0~(m-1)>" is the accessname for stream "1" to stream "m". Please refer to the "subgroup of network: rtsp" for setting the accessname of SDP.

You can get the SDP by HTTP GET.

When using scalable multicast, Get SDP file which contains the multicast information via HTTP.

6.21 Open the Network Stream

Note: This request requires Viewer access privileges.

Syntax:

For HTTP push server (MJPEG):

http://<*servername*>/<network_http_s<0~m-1>_accessname>

For RTSP (MP4), the user needs to input the URL below into an RTSP compatible player.

rtsp://<*servername*>/<network_rtsp_s<0~m-1>_accessname>

"m" is the stream number.

For details on streaming protocol, please refer to the "control signaling" and "data format" documents.

6.22 Senddata (capability.nuart>0)

Note: This request requires Viewer privileges.

Method: GET/POST

Syntax:

http://<*servername*>/cgi-bin/viewer/senddata.cgi? [com=<value>][&data=<value>][&flush=<value>] [&wait=<value>] [&read=<value>]

PARAMETER	VALUE	DESCRIPTION
com	1 ~ <max. com port number>	The target COM/RS485 port number.
data	<hex decimal data>[,<hex decimal data>]	The <hex decimal data> is a series of digits from 0 ~ 9, A ~ F. Each comma separates the commands by 200 milliseconds.
flush	yes,no	yes: Receive data buffer of the COM port will be cleared before read. no: Do not clear the receive data buffer.
wait	*1 ~ 65535*	Wait time in milliseconds before read data.
read	*1 ~ 128*	The data length in bytes to read. The read data will be in the return page.

Return:

```
HTTP/1.0 200 OK\r\n
Content-Type: text/plain\r\n
Content-Length: <system information length>\r\n
\r\n
<hex decimal data>\r\n
```

Where hexadecimal data is digits from 0 ~ 9, A ~ F.

6.23 Storage Managements (capability.storage.dbenabled=1)

Note: This request requires administrator privileges.

Method: GET and POST

Syntax:

```
http://<servername>/cgi-bin/admin/lsctrl.cgi?cmd=<cmd_type>[&<parameter>=<value>...]
```

The commands usage and their input arguments are as follows.

PARAMETER	VALUE	DESCRIPTION
cmd_type	<string>	Required. Command to be executed, including *search*, *insert*, *delete*, *update*, and *queryStatus*.

Command: **search**

PARAMETER	VALUE	DESCRIPTION
label	<integer primary key>	Optional. The integer primary key column will automatically be assigned a unique integer.
triggerType	<text>	Optional. Indicate the event trigger type. Please embrace your input value with single quotes. Ex. mediaType='motion' Support trigger types are product dependent.
mediaType	<text>	Optional. Indicate the file media type. Please embrace your input value with single quotes. Ex. mediaType='videoclip' Support trigger types are product dependent.
destPath	<text>	Optional. Indicate the file location in camera. Please embrace your input value with single quotes. Ex. destPath ='/mnt/auto/CF/NCMF/abc.mp4'

resolution	<text>	Optional. Indicate the media file resolution. Please embrace your input value with single quotes. Ex. resolution='800x600'
isLocked	<boolean>	Optional. Indicate if the file is locked or not. 0: file is not locked. 1: file is locked. A locked file would not be removed from UI or cyclic storage.
triggerTime	<text>	Optional. Indicate the event trigger time. (not the file created time) Format is "YYYY-MM-DD HH:MM:SS" Please embrace your input value with single quotes. Ex. triggerTime='2008-01-01 00:00:00' If you want to search for a time period, please apply "TO" operation. Ex. triggerTime='2008-01-01 00:00:00'+TO+'2008-01-01 23:59:59' is to search for records from the start of Jan 1st 2008 to the end of Jan 1st 2008.
limit	<positive integer>	Optional. Limit the maximum number of returned search records.
offset	<positive integer>	Optional. Specifies how many rows to skip at the beginning of the matched records. Note that the offset keyword is used after limit keyword.

To increase the flexibility of search command, you may use "OR" connectors for logical "OR" search operations. Moreover, to search for a specific time period, you can use "TO" connector.
Ex. To search records triggered by motion or di or sequential and also triggered between 2008-01-01 00:00:00 and 2008-01-01 23:59:59.

```
http://<servername>/cgi-bin/admin/lsctrl.cgi?cmd=search&triggerType='motion'+OR+'di'+OR+'seq'&triggerTime='2008-01-01 00:00:00'+TO+'2008-01-01 23:59:59'
```

Command: **delete**

PARAMETER	VALUE	DESCRIPTION
label	<integer primary key>	Required. Identify the designated record. Ex. label=1

Ex. Delete records whose key numbers are 1, 4, and 8.

```
http://<servername>/cgi-bin/admin/lsctrl.cgi?cmd=delete&label=1&label=4&label=8
```

Command: **update**

PARAMETER	VALUE	DESCRIPTION
label	<integer primary key>	Required. Identify the designated record. Ex. label=1
isLocked	<boolean>	Required. Indicate if the file is locked or not.

Ex. Update records whose key numbers are 1 and 5 to be locked status.

http://<*servername*>/cgi-bin/admin/lsctrl.cgi?cmd=update&isLocked=1&label=1&label=5

Ex. Update records whose key numbers are 2 and 3 to be unlocked status.

http://<*servername*>/cgi-bin/admin/lsctrl.cgi?cmd=update&isLocked=0&label=2&label=3

Command: queryStatus

PARAMETER	VALUE	DESCRIPTION
retType	xml or javascript	Optional. Ex. retype=javascript The default return message is in XML format.

Ex. Query local storage status and call for javascript format return message.

http://<*servername*>/cgi-bin/admin/lsctrl.cgi?cmd=queryStatus&retType=javascript

Technical Specifications

System
- CPU: Mozart 120 SoC
- Flash: 16MB
- RAM: 128MB + 128MB
- Embedded OS: Linux 2.6

Lens
- Board lens, vari-focal, f = 3 ~ 9 mm, F1.2 (wide), F2.1 (tele), auto-iris
- Removable IR-cut filter for day & night function

Angle of View
- 31.7° ~ 93.0° (horizontal)
- 23.8° ~ 68.4° (vertical)

Shutter Time
- 1/5 sec. to 1/40,000 sec.

Image Sensor
- 1/3.2" CMOS sensor in 1600x1200 resolution

Minimum Illumination
- 0.1 Lux / F1.2
- 0 Lux / F1.2 (IR LED on)

IR Illuminators
- Built-in IR illuminators, effective up to 25 meters

Video
- Compression: MJPEG & MPEG-4
- Streaming:
  Simultaneous multiple streams
  MPEG-4 streaming over UDP, TCP, HTTP or HTTPS
  MPEG-4 multicast streaming
  MJPEG streaming over HTTP or HTTPS
- Supports activity adaptive streaming for dynamic frame rate control
- Supports video cropping for bandwidth saving
- Supports ePTZ for data efficiency
- Supports 3GPP mobile surveillance
- Frame rates:
  MPEG-4: up to 30 fps at 800x600
  up to 10 fps at 1600x1200
  MJPEG: up to 30 fps at 800x600
  up to 15 fps at 1600x1200

Image Settings
- Adjustable image size, quality, and bit rate
- Time stamp and text caption overlay
- Flip & mirror
- Configurable brightness, contrast, saturation, sharpness, white balance and exposure
- AGC, AWB, AES
- Automatic, manual, or scheduled day/night mode
- BLC (Backlight Compensation)
- Supports privacy masks

Audio
- Compression:
  GSM-AMR speech encoding, bit rate: 4.75 kbps to 12.2 kbps
  MPEG-4 AAC audio encoding, bit rate: 16 kbps to 128 kbps
- Interface:
  External microphone input
  Audio output
- Supports two-way audio via SIP protocol
- Supports audio mute

Networking
- 10/100 Mbps Ethernet, RJ-45
- Protocols: IPv4, IPv6, TCP/IP, HTTP, HTTPS, UPnP, RTSP/RTP/RTCP, IGMP, SMTP, FTP, DHCP, NTP, DNS, DDNS, PPPoE, CoS, QoS, SNMP and 802.1X

Alarm and Event Management
- Triple-window video motion detection
- Tamper detection
- One D/I and one D/O for external sensor and alarm
- Event notification using HTTP, SMTP or FTP
- Local recording of MP4 file

On-board Storage
- SD/SDHC card slot
- Stores snapshots and video clips

Security
- Multi-level user access with password protection
- IP address filtering
- HTTPS encrypted data transmission
- 802.1X port-based authentication for network protection

Users
- Live viewing for up to 10 clients

Dimension
- Φ83x210mm

Weight
- Net: 1600g (Including bracket)

LED Indicator
- System restore status indicator

Power
- 12V DC
- 24V AC
- Power consumption: Max. 7 W
- 802.3af compliant Power-over-Ethernet

Housing
- Weather-proof IP67-rated housing

Approvals
- CE, LVD, FCC, VCCI, C-Tick

Operating Environments
- Temperature: -20 ~ 50 °C (-4 ~ 122 °F)
- Humidity: 90% RH

Viewing System Requirements
- OS: Microsoft Windows 2000/XP/Vista
- Browser: Mozilla Firefox, Internet Explorer 6.x or above
- Cell phone: 3GPP player
- Real Player: 10.5 or above
- Quick Time: 6.5 or above

Installation, Management, and Maintenance
- Mounting bracket w/ cable concealment
- RS-485 interface for scanners, pan/tilts
- Installation Wizard 2
- 32-CH ST7501 central management software
- Supports firmware upgrade

Applications
- SDK available for application development and system integration

Warranty
- 24 months

All specifications are subject to change without notice. Copyright©2009 VIVOTEK INC. All rights reserved.

Technology License Notice

MPEG-4 AAC Technology

THIS PRODUCT IS LICENSED UNDER THE MPEG-4 AAC AUDIO PATENT LICENSE. THIS PRODUCT MAY NOT BE DECOMPILED, REVERSE-ENGINEERED OR COPIED, EXCEPT WITH REGARD TO PC SOFTWARE, OF WHICH YOU MAY MAKE SINGLE COPIES FOR ARCHIVAL PURPOSES. FOR MORE INFORMATION, PLEASE REFER TO HTTP://WWW.VIALICENSING.COM.

MPEG-4 Visual Technology

THIS PRODUCT IS LICENSED UNDER THE MPEG-4 VISUAL PATENT PORTFOLIO LICENSE FOR THE PERSONAL AND NON-COMMERCIAL USE OF A CONSUMER FOR (i) ENCODING VIDEO IN COMPLIANCE WITH THE MPEG-4 VISUAL STANDARD ("MPEG-4 VIDEO") AND/OR (ii) DECODING MPEG-4 VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL AND NON-COMMERCIAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED BY MPEG LA TO PROVIDE MPEG-4 VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION INCLUDING THAT RELATING TO PROMOTIONAL, INTERNAL AND COMMERCIAL USES AND LICENSING MAY BE OBTAINED FROM MPEG LA, LLC. PLEASE REFER TO HTTP://WWW.MPEGLA.COM.

AMR-NB Standard

THIS PRODUCT IS LICENSED UNDER THE AMR-NB STANDARD PATENT LICENSE AGREEMENT. WITH RESPECT TO THE USE OF THIS PRODUCT, THE FOLLOWING LICENSORS' PATENTS MAY APPLY:

TELEFONAKIEBOLAGET ERICSSON AB: US PAT. 6192335; 6275798; 6029125; 6424938; 6058359. NOKIA CORPORATION: US PAT. 5946651; 6199035. VOICEAGE CORPORATION: AT PAT. 0516621; BE PAT. 0516621; CA PAT. 2010830; CH PAT. 0516621; DE PAT. 0516621; DK PAT. 0516621; ES PAT. 0516621; FR PAT. 0516621; GB PAT. 0516621; GR PAT. 0516621; IT PAT. 0516621; LI PAT. 0516621; LU PAT. 0516621; NL PAT. 0516621; SE PAT 0516621; US PAT 5444816; AT PAT. 819303/AT E 198805T1; AU PAT. 697256; BE PAT. 819303; BR PAT. 9604838-7; CA PAT. 2216315; CH PAT. 819303; CN PAT. ZL96193827.7; DE PAT. 819303/DE69611607T2; DK PAT. 819303; ES PAT. 819303; EP PAT. 819303; FR PAT. 819303; GB PAT. 819303; IT PAT. 819303; JP PAT. APP. 8-529817; NL PAT. 819303; SE PAT. 819303; US PAT. 5664053. THE LIST MAY BE UPDATED FROM TIME TO TIME BY LICENSORS AND A CURRENT VERSION OF WHICH IS AVAILABLE ON LICENSOR'S WEBSITE AT HTTP://WWW.VOICEAGE.COM.

Electromagnetic Compatibility (EMC)

FCC Statement

This device compiles with FCC Rules Part 15. Operation is subject to the following two conditions.

- This device may not cause harmful interference, and
- This device must accept any interference received, including interference that may cause undesired operation.

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the installation manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case the user will be required to correct the interference at his own expense.

CE Mark Warning CE

This is a Class A product. In a domestic environment, this product may cause radio interference, in which case the user may be required to take adequate measures.

Liability

VIVOTEK Inc. cannot be held responsible for any technical or typographical errors and reserves the right to make changes to the product and manuals without prior notice. VIVOTEK Inc. makes no warranty of any kind with regard to the material contained within this document, including, but not limited to, the implied warranties of merchantability and fitness for any particular purpose.